PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-162506**
(43)Date of publication of application : **06.06.2003**

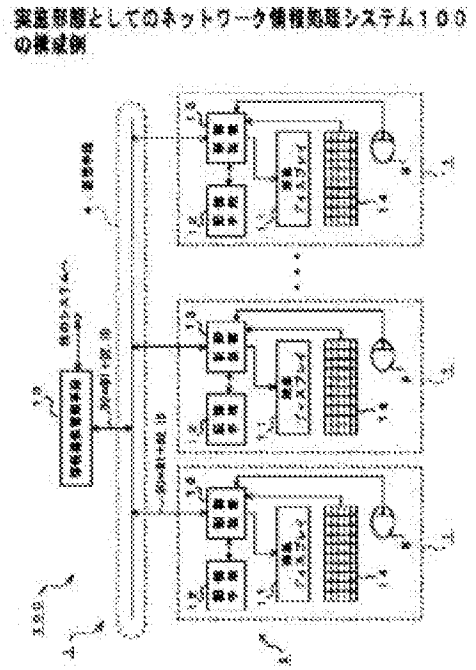
(51)Int.Cl. G06F 15/00
G06F 1/00
G06T 1/00
H04N 7/173

(21)Application number : **2001-358041**
(22)Date of filing : **22.11.2001**

(71)Applicant : **SONY CORP**
(72)Inventor : **ISOZAKI MASAAKI**

(54) NETWORK INFORMATION PROCESSING SYSTEM, INFORMATION- PROVIDING MANAGEMENT APPARATUS, INFORMATION-PROCESSING APPARATUS AND INFORMATION-PROCESSING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To reject participation by unauthorized users to a system and preventing electronic equipment for a network configuration including an information providing management group from unauthorized use by a third party.
SOLUTION: A network information processing system 100 comprising more than one information processing apparatus 1, having a GUI (graphical user interface) function to process any information, an information providing management means 10 processing information transmitted from the processing apparatuses 1 to provide electronic information contents and a communication means 4 connecting the management means 10 to each processing apparatus 1, where authentication processing to authenticate personal identification, by using the GUI function of the processing apparatuses 1. For example, if personal information read out from face image information D1 does not match the personal information presented from the third party, the system 100 can reject the participation in the system 100.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－162506
（P2003－162506A）
(43)公開日　平成15年６月６日(2003.6.6)

(51)Int.Cl.[7]		識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｂ　５Ｂ０５７
	1/00	３７０		1/00	３７０Ｅ　５Ｂ０８５
Ｇ０６Ｔ	1/00	５００	Ｇ０６Ｔ	1/00	５００Ｂ　５Ｃ０６４
Ｈ０４Ｎ	7/173	６４０	Ｈ０４Ｎ	7/173	６４０Ｚ

審査請求　有　　請求項の数35　ＯＬ　（全 22 頁）

(21)出願番号　特願2001－358041(P2001－358041)

(22)出願日　平成13年11月22日(2001.11.22)

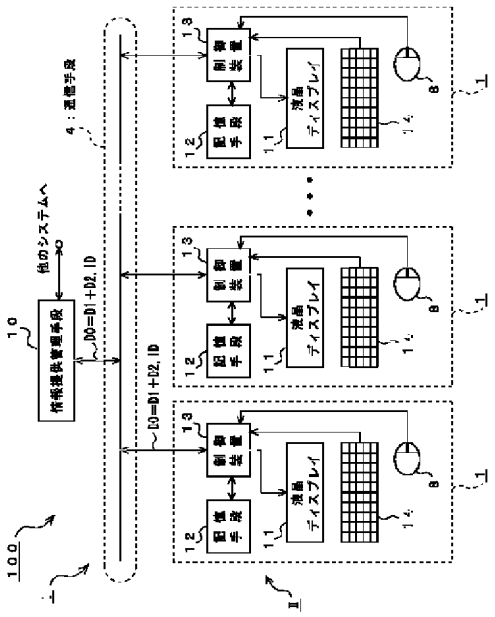
(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　五十崎　正明
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100090376
弁理士　山口　邦夫　（外１名）

最終頁に続く

(54)【発明の名称】　ネットワーク情報処理システム、情報提供管理装置、情報処理装置及び情報処理方法

(57)【要約】
【課題】　不正使用者の当該システムへの参加を拒否できるようにすると共に、当該情報提供管理系を含むネットワーク構成用の電子機器の第三者による不正使用を防止できるようにする。
【解決手段】　ＧＵＩ機能を有して任意の情報を処理する一以上の情報処理装置１と、少なくとも、情報処理装置１から転送される情報を処理し表示情報を含む電子情報内容を提供する情報提供管理手段１０と、この情報提供管理手段１０と各々の情報処理装置１とを接続する通信手段４とを備え、情報提供管理手段１０又は情報処理装置１において、当該情報処理装置１のＧＵＩ機能を利用して使用者本人を特定するための認証処理をするようにしたものである。例えば、顔画像情報Ｄ１から読み出した個人情報と、第三者から提示された個人情報とが一致しない場合は当該システム１００への参加を拒否することができる。

実施形態としてのネットワーク情報処理システム１００の構成例



【特許請求の範囲】
【請求項１】　複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムであって、
入力操作機能を有して任意の情報を処理する一以上の情報処理装置と、
少なくとも、前記情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する情報提供管理手段と、
前記情報提供管理手段と各々の前記情報処理装置とを接続する通信手段とを備え、
前記情報提供管理手段又は情報処理装置において、当該情報処理装置の入力操作機能を利用して使用者本人を特定するための認証処理をするようにしたことを特徴とするネットワーク情報処理システム。
【請求項２】　前記情報提供管理手段において使用者本人を認証処理する場合であって、
予め前記情報処理装置から前記情報提供管理手段へ使用者の顔画像情報及び個人情報を登録請求し、
前記情報提供管理手段では、
前記情報処理装置によって登録された使用者の顔画像情報に個人情報を付加して管理すると共に、前記使用者の情報処理装置に対して登録済みを示すキー情報を配信し、
以後、前記情報提供管理手段に対して前記入力操作機能を利用して前記キー情報及び個人情報が提示されたとき、
前記情報提供管理手段では、
前記キー情報に基づいて前記顔画像情報から個人情報を読み出し、
読み出された前記個人情報と提示された個人情報とを比較照合して前記本人を認証するようにしたことを特徴とする請求項１に記載のネットワーク情報処理システム。
【請求項３】　前記情報処理装置において使用者本人を認証処理する場合であって、
予め前記情報処理装置から前記情報提供管理手段へ使用者の顔画像情報及び個人情報を登録請求し、
前記情報提供管理手段では、
前記情報処理装置によって登録された使用者の顔画像情報に個人情報を付加した使用者顔画像情報を作成すると共に、前記使用者の情報処理装置に対して前記使用者顔画像情報及び登録済みを示すキー情報を配信し、
以後、前記情報処理装置に対して当該入力操作機能を利用して前記キー情報が入力されたとき、
前記情報処理装置では、
前記キー情報に基づいて前記使用者顔画像情報から個人情報を読み出し、
読み出された前記個人情報と提示された個人情報とを比較照合して前記本人を認証するようにしたことを特徴とする請求項１に記載のネットワーク情報処理システム。
【請求項４】　前記使用者の顔画像内に本人を特定する個人情報を重畳し、
前記顔画像内に重畳された個人情報を読み出して当該使用者本人を認証することを特徴とする請求項１に記載のネットワーク情報処理システム。
【請求項５】　前記情報提供管理手段を含むネットワーク構成用の電子機器を操作できる範囲を示した操作権情報が前記個人情報に付加されることを特徴とする請求項１に記載のネットワーク情報処理システム。
【請求項６】　前記個人情報は、
前記キー情報によって復号可能な情報に暗号化され、
前記暗号化後の個人情報を前記使用者の顔画像内の上下の所定ラインを表示する画像表示情報に重畳されることを特徴とする請求項１に記載のネットワーク情報処理システム。
【請求項７】　前記使用者顔画像情報を構成する画像表示情報にはチェック情報が含まれ、
前記使用者の認証時に、
前記チェック情報に基づいて前記画像表示情報の符号ビットを加算し、
前記符号ビットを加算した加算結果と前記チェック情報による期待加算結果とを比較照合することを特徴とする請求項３に記載のネットワーク情報処理システム。
【請求項８】　前記比較照合の結果で、前記符号ビットを加算した加算結果と前記チェック情報による加算結果とが一致しない場合は、
当該システムへの前記使用者の参加を拒否し、又は、前記情報提供管理手段を含むネットワーク構成用の電子機器の使用権利を制限することを特徴とする請求項７に記載のネットワーク情報処理システム。
【請求項９】　前記使用者顔画像情報は、
特定の管理者によって作成され、前記情報提供管理手段へ登録し及び使用者の情報処理装置に発行するようになされることを特徴とする請求項３に記載のネットワーク情報処理システム。
【請求項１０】　前記情報処理装置を不特定多数の使用者により共通に操作する場合は、
予め前記情報提供管理手段へ登録しておいた自分の使用者顔画像情報を当該情報処理装置にダウンロードして使用することを特徴とする請求項３に記載のネットワーク情報処理システム。
【請求項１１】　前記情報処理装置に表示手段が設けられ、
前記使用者の顔画像に付加された個人情報を前記入力操作機能を利用して表示することを特徴とする請求項１に記載のネットワーク情報処理システム。
【請求項１２】　前記使用者が未認証である場合は、
前記表示手段には当該使用者が未認証である旨の表示がなされることを特徴とする請求項１に記載のネットワーク情報処理システム。

【請求項１３】　少なくとも、使用者の情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する装置であって、
前記情報処理装置から登録された使用者の顔画像情報及び個人情報を記憶する記憶手段と、
前記情報処理装置によって登録請求された使用者の顔画像情報に個人情報を付加して管理すると共に、前記使用者の情報処理装置に対して登録済みを示すキー情報を配信する制御装置とを備え、
当該制御装置に対して前記情報処理装置から前記キー情報が提示されたとき、
前記キー情報に基づいて前記顔画像情報から個人情報を読み出し、
読み出された前記個人情報と提示された個人情報とを比較照合して前記本人を認証するようにしたことを特徴とする情報提供管理装置。
【請求項１４】　少なくとも、使用者の情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する装置であって、
前記情報処理装置から登録請求された使用者の顔画像情報及び個人情報を記憶する記憶手段と、
前記情報処理装置によって登録請求された使用者の顔画像情報に個人情報を付加した使用者顔画像情報を作成すると共に、前記使用者顔画像情報及び登録済みを示すキー情報を前記使用者の情報処理装置に配信する制御装置とを備えることを特徴とする情報提供管理装置。
【請求項１５】　前記使用者の顔画像内に本人を特定する個人情報を重畳し、
前記顔画像内に重畳された個人情報を読み出して当該使用者本人を認証することを特徴とする請求項１４に記載の情報提供管理装置。
【請求項１６】　前記個人情報は、
前記キー情報によって復号可能な情報に暗号化され、
前記暗号化後の個人情報を前記使用者の顔画像内の上下の所定ラインを表示する画像表示情報に重畳されることを特徴とする請求項１４に記載の情報提供管理装置。
【請求項１７】　前記使用者顔画像情報を構成する画像表示情報にはチェック情報が含まれ、前記使用者の認証時に、
前記チェック情報に基づいて前記画像表示情報の符号ビットを加算し、
前記符号ビットを加算した加算結果と前記チェック情報による期待加算結果とを比較照合することを特徴とする請求項１４に記載の情報提供管理装置。
【請求項１８】　前記比較照合の結果で、前記符号ビットを加算した加算結果と前記チェック情報による加算結果とが一致しない場合は、
当該システムへの前記使用者の参加を拒否し、又は、前記情報提供管理手段を含むネットワーク構成用の電子機器の使用権利を制限することを特徴とする請求項１７に記載の情報提供管理装置。
【請求項１９】　前記使用者顔画像情報は、
特定の管理者によって作成され、前記情報提供管理手段へ登録し及び使用者の情報処理装置に発行するようになされることを特徴とする請求項１４に記載の情報提供管理装置。
【請求項２０】　使用者本人を認証するためのキー情報に基づいて任意の情報を処理する装置であって、
前記キー情報を入力する入力手段と、
予め取得された使用者顔画像情報及び登録済みを示すキー情報を記憶する記憶手段と、
前記入力手段により入力されたキー情報に基づいて前記記憶手段から使用者顔画像情報を読み出すと共に前記使用者顔画像情報から個人情報を読み出し、前記使用者顔画像情報から読み出された前記個人情報と前記入力手段により入力された個人情報とを比較照合して前記使用者本人を認証する制御装置とを備えることを特徴とする情報処理装置。
【請求項２１】　前記使用者の顔画像を表示する表示手段が備えられ、
前記使用者の顔画像に付加された個人情報を前記入力操作機能を利用して表示することを特徴とする請求項２０に記載の情報処理装置。
【請求項２２】　前記使用者が未認証である場合は、
前記表示手段には当該使用者が未認証である旨の表示がなされることを特徴とする請求項２０に記載の情報処理装置。
【請求項２３】　入力操作機能を有して任意の情報を処理する一以上の情報処理系と、少なくとも、前記情報処理系から転送される情報を処理し表示情報を含む電子情報内容を提供する情報提供管理系とを準備し、
前記情報提供管理系又は情報処理系において、当該情報処理系の入力操作機能を利用して使用者本人を特定するための認証処理をするようにしたことを特徴とする情報処理方法。
【請求項２４】　前記情報処理系と前記情報提供管理系とを通信手段により接続することを特徴とする請求項２３に記載の情報処理方法。
【請求項２５】　前記情報提供管理系において使用者本人の認証処理をする場合であって、
前記情報処理系から前記情報提供管理系へ使用者の顔画像及び個人情報を登録請求し、
前記情報管理提供系では、
前記情報処理系によって登録請求された使用者の顔画像に個人情報を付加して管理すると共に、前記使用者に対して登録済みを示すキー情報を配信し、
以後、前記情報管理提供系に対して前記キー情報が提示されたとき、
前記情報管理提供系では、
前記キー情報に基づいて前記顔画像から個人情報を読み

出し、
読み出された前記個人情報と提示された個人情報とを比較照合して前記本人を認証するようにしたことを特徴とする請求項２３に記載の情報処理方法。
【請求項２６】　前記情報処理系において使用者本人の認証処理をする場合であって、
前記情報処理系から前記情報提供管理系へ使用者の顔画像及び個人情報を登録請求し、
前記情報管理提供系では、
前記情報処理系によって登録請求された使用者の顔画像に個人情報を付加して使用者顔画像情報を作成すると共に、前記使用者に対して使用者顔画像情報及び登録済みを示すキー情報を配信し、
以後、前記情報処理系に対して前記キー情報が提示されたとき、
前記情報処理系では、
前記キー情報に基づいて前記使用者顔画像情報から個人情報を読み出し、
読み出された前記個人情報と提示された個人情報とを比較照合して前記本人を認証するようにしたことを特徴とする請求項２３に記載の情報処理方法。
【請求項２７】　前記使用者の顔画像内に本人を特定する個人情報を重畳し、
前記顔画像内に重畳された個人情報を読み出して当該使用者本人を認証することを特徴とする請求項２３に記載の情報処理方法。
【請求項２８】　前記情報提供管理系を含むネットワーク構成用の電子機器を操作できる範囲を示した操作権情報を前記個人情報に付加することを特徴とする請求項２３に記載の情報処理方法。
【請求項２９】　前記個人情報は、
前記キー情報によって復号可能な情報に暗号化し、
前記暗号化後の個人情報を前記使用者の顔画像内の上下の所定ラインを表示する画像表示情報に重畳することを特徴とする請求項２３に記載の情報処理方法。
【請求項３０】　前記使用者顔画像情報を構成する画像表示情報にチェック情報を付加し、
前記使用者の認証時には、
前記チェック情報に基づいて前記画像表示情報の符号ビットを加算し、
前記符号ビットを加算した加算結果と前記チェック情報による期待加算結果とを比較照合することを特徴とする請求項２６に記載の情報処理方法。
【請求項３１】　前記比較照合の結果で、前記符号ビットを加算した加算結果と前記チェック情報による加算結果とが一致しない場合は、
当該システムへの前記使用者の参加を拒否し、又は、前記情報提供管理手段を含むネットワーク構成用の電子機器の使用権利を制限することを特徴とする請求項３０に記載の情報処理方法。
【請求項３２】　前記使用者顔画像情報を特定の管理者によって作成し、
前記情報提供管理系へ該使用者顔画像情報を登録すると共に、前記使用者顔画像情報を使用者の情報処理系に発行するようにしたことを特徴とする請求項２６に記載の情報処理方法。
【請求項３３】　前記情報処理系を不特定多数の使用者により共通に操作する場合は、
予め前記情報提供管理系へ登録しておいた自分の使用者顔画像情報を当該情報処理系にダウンロードして使用することを特徴とする請求項２３に記載の情報処理方法。
【請求項３４】　前記情報処理系に表示手段を設け、
前記使用者の顔画像に付加された個人情報を前記情報処理系の入力操作機能を利用して表示することを特徴とする請求項２３に記載の情報処理方法。
【請求項３５】　前記使用者が未認証である場合は、
前記表示手段には当該使用者が未認証である旨の表示をすることを特徴とする請求項３４に記載の情報処理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワーク会議システムや、ネットワーク教育システム、ネットワークゲームシステム等に適用して好適なネットワーク情報処理システム、情報提供管理装置、情報処理装置及び情報処理方法に関する。
【０００２】詳しくは、任意の情報を処理する一以上の情報処理装置と、表示情報を含む電子情報内容を提供する情報提供管理手段とを通信手段により接続し、情報提供管理手段又は情報処理装置において、当該情報処理装置の入力操作機能を利用して使用者本人を特定するための認証処理をし、不正使用者の当該システムへの参加を拒否できるようにすると共に、当該情報提供管理手段を含むネットワーク構成用の電子機器の第三者による不正使用を防止できるようにしたものである。
【０００３】
【従来の技術】近年、パーソナルコンピュータ（以下でパソコンという）を用いて作成したプレゼンテーション資料を会議室に持ち込んで、プレゼンタ（資料発表者）がそれを複数の会議参加者に対して電子機器を用いて発表する、いわゆる電子会議システムが採られる場合が多くなってきた。
【０００４】この電子会議システムでは表示機器と資料発表者のノートパソコンとが接続される。この表示機器にはデータプロジェクタが使用され、パソコンで作成したプレゼンテーション資料が表示される。データプロジェクタ（以下で単にプロジェクタという）には、一人のプレゼンタ自身のノートパソコンがＲＧＢケーブルを通じて接続され、そのノートパソコンに表示されている画面を白壁等に投影するようになされる。白壁等に表示さ

れているプレゼンテーション資料は発表者が操作するマウスカーソルによって指し示すようになされる。つまり、白壁等には説明者が所有している資料のみが表示される。

【０００５】最近では、ネットワーク対応のデータプロジェクタが登場している。このプロジェクタにはパソコン機能が内蔵されているものである。これによれば、説明者が自身のノートパソコン（以下で情報処理装置ともいう）からプレゼンテーションファイルをネットワーク経由でプロジェクタに転送し、そのプロジェクタのパソコン機能によりその内容を表示し投影するようになされる。

【０００６】

【発明が解決しようとする課題】ところで、従来例に係る電子会議システムによれば、以下のような問題がある。

① ネットワーク構成用の電子機器の第三者による不正使用を防止しようとしたとき、当該電子会議システムにおいて、クライアント側の情報処理装置の画面上に参加者の顔写真等のユーザアイコンを表示し、当該システムへの参加許否を判別する方法が考えられる。

【０００７】この場合、ユーザアイコンの作成及び登録を参加者側に自由に委ねてしまうと、第三者が不正に他人のユーザアイコンを使用して、当該電子会議に参加してしまうおそれがある。特に、参加者が支社から本社へ出向していたり、別の会議場所に居る場合などは、お互いの顔を確認し合うことができない場合が多い。このような場合に第三者が本人になりすまして会議に参加し、貴重なプレゼンテーション情報を盗用してしまうことが予想される。

【０００８】② 当該電子会議システムにおいて、ユーザアイコンをクリックして相手を指定し、チャットやファイル転送等を行うような操作を導入しようとした場合に、なりすまし参加者相手に、誤ってチャットやファイルを転送しまうおそれがある。従って、貴重なプレゼンテーション情報が漏洩してしまう危険性が高くなり、セキュリティ上で大きな問題となる。特に、不特定多数のユーザが共通のノートパソコンを情報処理装置として使用する場合には、ユーザアイコンの管理が益々重要になってくる。

【０００９】そこで、この発明はこのような従来の課題を解決したものであって、不正使用者の当該システムへの参加を拒否できるようにすると共に、当該情報提供管理系を含むネットワーク構成用の電子機器の第三者による不正使用を防止できるようにしたネットワーク情報処理システム、情報提供管理装置、情報処理装置及び情報処理方法を提供することを目的とする。

【００１０】

【課題を解決するための手段】上述した課題は、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムであって、入力操作機能を有して任意の情報を処理する一以上の情報処理装置と、少なくとも、情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する情報提供管理手段と、この情報提供管理手段と各々の情報処理装置とを接続する通信手段とを備え、情報提供管理手段又は情報処理装置において、当該情報処理装置の入力操作機能を利用して使用者本人を特定するための認証処理をするようにしたことを特徴とするネットワーク情報処理システムによって解決される。

【００１１】本発明に係るネットワーク情報処理システムによれば、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される場合であって、一以上の情報処理装置と情報提供管理手段とが通信手段により接続され、情報提供管理手段では、情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供するようになされる。これを前提にして、当該システムへの参加時等に情報提供管理手段又は情報処理装置において、当該情報処理装置の入力操作機能を利用して使用者本人を特定するための認証処理がなされる。

【００１２】例えば、情報提供管理手段において使用者本人を認証処理する場合であって、予め情報処理装置から情報提供管理手段へ使用者の顔画像情報及び個人情報が登録請求される。情報提供管理手段では情報処理装置によって登録請求された使用者の顔画像情報に個人情報を付加して管理すると共に、使用者の情報処理装置に対して登録済みを示すキー情報が配信される。

【００１３】以後、情報提供管理手段に対して情報処理装置の入力操作機能を利用してキー情報が提示されたとき、情報提供管理手段ではキー情報に基づいて顔画像情報から個人情報を読み出し、ここで読み出された個人情報と提示された個人情報とを比較照合して本人を認証するようになされる。

【００１４】従って、顔画像情報から読み出した個人情報と、使用者から提示された個人情報とが一致した場合は当該システムへの参加を許可することができる。また、顔画像情報から読み出した個人情報と、第三者から提示された個人情報とが一致しない場合は当該システムへの参加を拒否することができる。これにより、情報提供管理手段又は情報処理装置において、当該情報提供管理手段を含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

【００１５】本発明に係る第１の情報提供管理装置は少なくとも、使用者の情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する装置であって、情報処理装置から登録請求された使用者の顔画像情報及び個人情報を記憶する記憶手段と、この情報処理装置によって登録請求された使用者の顔画像情報に個人情報を付加して管理すると共に、使用者の情報処理装置に対して登録済みを示すキー情報を配信する制御装置と

を備え、当該制御装置に対して情報処理装置からキー情報が提示されたとき、キー情報に基づいて顔画像情報から個人情報を読み出し、ここで読み出された個人情報と提示された個人情報とを比較照合して本人を認証するようにしたことを特徴とするものである。

【００１６】本発明に係る第１の情報提供管理装置によれば、少なくとも、使用者の情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する場合に、記憶手段には情報処理装置から登録請求された使用者の顔画像情報及び個人情報が記憶される。制御装置では使用者の顔画像情報に個人情報を付加して管理すると共に、この使用者の情報処理装置に対して登録済みを示すキー情報が配信される。これを前提にして、当該制御装置に対して情報処理装置からキー情報が提示されると、この制御装置ではキー情報に基づいて顔画像情報から読み出した個人情報と、提示された個人情報とを比較照合して本人を認証するようになされる。

【００１７】従って、当該情報提供管理装置において使用者本人を認証処理することができる。これにより、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムに対して第１の情報提供管理装置を十分応用することができる。

【００１８】本発明に係る第２の情報提供管理装置は少なくとも、使用者の情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する装置であって、情報処理装置から登録請求された使用者の顔画像情報及び個人情報を記憶する記憶手段と、この情報処理装置によって登録請求された使用者の顔画像情報に個人情報を付加した使用者顔画像情報を作成すると共に、使用者顔画像情報及び登録済みを示すキー情報を使用者の情報処理装置に配信する制御装置とを備えることを特徴とするものである。

【００１９】本発明に係る第２の情報提供管理装置によれば、少なくとも、使用者の情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する場合に、記憶手段には情報処理装置から登録請求された使用者の顔画像情報及び個人情報が記憶される。制御装置では使用者の顔画像情報に個人情報を付加して使用者顔画像情報を作成すると共に、この使用者顔画像情報及び登録済みを示すキー情報が使用者の情報処理装置に配信される。

【００２０】従って、当該情報処理装置においてキー情報に基づき使用者顔画像情報から読み出した個人情報と、提示された個人情報とを比較照合して本人を認証することができる。これにより、情報処理装置側で使用者本人を認証できることから、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムに対して第２の情報提供管理装置を十分応用することができる。

【００２１】本発明に係る情報処理装置は使用者本人を認証するためのキー情報に基づいて任意の情報を処理する装置であって、キー情報を入力する入力手段と、予め取得された使用者顔画像情報及び登録済みを示すキー情報を記憶する記憶手段と、入力手段により入力されたキー情報に基づいて記憶手段から使用者顔画像情報を読み出すと共に使用者顔画像情報から個人情報を読み出し、使用者顔画像情報から読み出された個人情報と入力手段により入力された個人情報とを比較照合して使用者本人を認証する制御装置とを備えることを特徴とするものである。

【００２２】本発明に係る情報処理装置によれば、使用者本人を認証するためのキー情報に基づいて任意の情報を処理する場合に、入力手段を使用してキー情報が入力される。予め取得された使用者顔画像情報及び登録済みを示すキー情報が記憶手段に記憶されている。これを前提にして、制御装置ではキー情報に基づいて使用者顔画像情報から個人情報を読み出し、この使用者顔画像情報から読み出された個人情報と入力手段により入力された個人情報とを比較照合するようになされる。

【００２３】従って、当該情報処理装置において使用者本人を認証することができる。これにより、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムに対して当該情報処理装置を十分応用することができる。

【００２４】本発明に係る情報処理方法は入力操作機能を有して任意の情報を処理する一以上の情報処理系と、少なくとも、情報処理系から転送される情報を処理し表示情報を含む電子情報内容を提供する情報提供管理系とを準備し、情報提供管理系又は情報処理系において、当該情報処理系の入力操作機能を利用して使用者本人を特定するための認証処理をするようにしたことを特徴とするものである。

【００２５】本発明に係る情報処理方法によれば、顔画像情報から読み出した個人情報と、使用者から提示された個人情報とが一致した場合は当該システムへの参加を許可することができる。また、顔画像情報から読み出した個人情報と、第三者から提示された個人情報とが一致しない場合は当該システムへの参加を拒否することができる。これにより、情報提供管理系又は情報処理系において、当該情報提供管理系を含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

【００２６】

【発明の実施の形態】続いて、この発明に係るネットワーク情報処理システム、情報提供管理装置、情報処理装置及び情報処理方法の一実施の形態について、図面を参照しながら説明をする。

【００２７】（１）実施形態

図１は本発明に係る実施形態としてのネットワーク情報処理システム１００の構成例を示すブロック図である。この実施形態では任意の情報を処理する一以上の情報処

理装置と、表示情報を含む電子情報内容を提供する情報提供管理手段とを通信手段により接続し、情報提供管理手段又は情報処理装置において、当該情報処理装置の入力操作機能を利用して使用者本人を特定するための認証処理をし、顔画像情報から読み出した個人情報と、使用者から提示された個人情報とが一致しない場合は当該システムへの参加を拒否できるようにすると共に、当該情報提供管理手段を含むネットワーク構成用の電子機器の第三者による不正使用を防止できるようにしたものである。

【００２８】図１に示すネットワーク情報処理システムは、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムであり、ネットワーク会議システムや、ネットワーク教育システム、ネットワークゲームシステム等に適用して好適なものである。

【００２９】当該システム１００は特定の領域又は会議室等の特定の場所に情報提供管理手段１０（情報提供管理系Ｉ）を配置すると共に、その特定の領域又は特定の場所内に一以上の情報処理装置１（情報処理系II）を準備し、この情報提供管理手段１０と各々の情報処理装置１とを通信手段４により接続し、これらの情報処理装置１から操作指示に基づいて情報提供管理手段１０を遠隔制御するようになされる。情報提供管理手段１０は他のネットワーク情報処理システムと接続して使用してもよい。遠隔地間会議システム等を構築することができる。

【００３０】このシステム１００では情報提供管理手段１０又は情報処理装置１において、当該情報処理装置１の入力操作機能を利用して使用者本人を特定するための認証処理をするようにした。例えば、情報提供管理手段１０では使用者顔画像情報Ｄ０を作成するようになされる。使用者顔画像情報Ｄ０とは情報処理装置１によって登録請求された使用者の顔画像情報Ｄ１に個人情報Ｄ２を付加したものをいう。個人情報Ｄ２とは、使用者の名前、社員番号、メールアドレス、電話番号等をいう。

【００３１】このシステム１００で使用者顔画像情報Ｄ０は特定の管理者によって作成され、情報提供管理手段１０等へ登録し及び使用者の情報処理装置１に発行するようになされる。発行先立ち、情報提供管理手段１０では使用者の顔画像内に本人を特定する個人情報Ｄ２を重畳し、使用時には顔画像内に重畳された個人情報Ｄ２を読み出して当該使用者本人を認証するようになされる。こうすることで、第三者が容易に使用者顔画像情報Ｄ０を不正使用することができなくなる。

【００３２】情報処理装置１はキー情報ＩＤに基づいて任意の情報を処理する装置である。キー情報ＩＤには使用者本人を認証するためパスワードが使用される。情報処理装置１には入力手段の一例となるキーボード１４及びマウス８が備えられている。キーボード１４はキー情報ＩＤや、グループ識別情報等を入力する際に使用される。当該システム１００を終了する際にはエグジットキー等を押下するようになされる。マウス８はファイル転送時等においてポインタ操作する際に使用される。キーボード１４及びマウス８には制御装置１３が接続されている。

【００３３】この制御装置１３には記憶手段１２が接続され、予め取得された使用者顔画像情報Ｄ０及び登録済みを示すキー情報ＩＤを記憶するようになされる。制御装置１３ではキーボード１４により入力されたキー情報ＩＤに基づいて記憶手段１２から使用者顔画像情報Ｄ０を読み出すと共に使用者顔画像情報Ｄ０から個人情報Ｄ２を読み出し、使用者顔画像情報Ｄ０から読み出された個人情報Ｄ２とキーボード１４により入力された個人情報Ｄ２とを比較照合して使用者本人を認証するようになされる。

【００３４】この制御装置１３には表示手段の一例となる液晶ディスプレイ１１が接続されており、使用者の顔画像を表示するようになされる。液晶ディスプレイ１１には入力操作機能の一例となるグラフィックユーザインタフェース（以下でＧＵＩ機能という）を有しており、このＧＵＩ機能及びマウス操作機能を利用して任意の情報を処理するようになされる。

【００３５】液晶ディスプレイ１１には使用者の顔画像に付加された個人情報Ｄ２をＧＵＩ機能を利用して表示される。ここでＧＵＩ機能を利用した入力操作とはマウス８の右クリック等の操作をいう。このようにすると、他の参加者が該当する使用者顔画像の所有者の個人情報Ｄ２を容易に確認することができる。このシステム１００で使用者が未認証である場合は、液晶ディスプレイ１１には当該使用者が未認証である旨の表示がなされる。

【００３６】情報処理装置１には持ち運び便利なノート型のパーソナルコンピュータが使用される。電子会議システム等に参加する場合には専用のアプリケーション（クライアントＧＵＩプログラム等）が予め情報処理装置１にインストールされる。情報提供管理手段１０では少なくとも、この情報処理装置１から転送される情報を処理し表示情報を含む電子情報内容を提供するようになされる。

【００３７】なお、システム１００で情報処理装置１を不特定多数の使用者により共通に操作する場合は予め情報提供管理手段１０へ登録しておいた自分の使用者顔画像情報Ｄ０を当該情報処理装置１にダウンロードして使用するようになされる。

【００３８】続いて、本発明に係る実施形態としての情報処理方法について当該システム１００における認証処理例について説明をする。この実施形態ではＧＵＩ機能を有して任意の情報を処理する一以上の情報処理系II と、少なくとも、情報処理系IIから転送される情報を処理し表示情報を含む電子情報内容を提供する情報提供管理系Ｉとを準備し、情報提供管理系Ｉ又は情報処理系II

において、当該情報処理系IIのＧＵＩ機能を利用して使用者本人を特定するための認証処理をする場合を前提とする。

【００３９】このシステム１００では

①　情報提供管理系Ｉにおいて、当該情報処理系IIのＧＵＩ機能を利用して使用者本人を特定するための認証処理をする場合、及び、

②　情報処理系IIにおいて、当該情報処理系IIのＧＵＩ機能を利用して使用者本人を特定するための認証処理をする場合について分けて説明をする。もちろん、情報処理装置１と情報提供管理手段１０とが通信手段４により接続されていることが好ましいが、登録済みを示すキー情報ＩＤは記憶媒体（例えばＣＤ－ＲＯＭ等）を利用して配布してもよい。

【００４０】［情報提供管理系Ｉで認証処理をする場合①］図２は、情報提供管理系Ｉにおける認証例を示すフローチャートである。このシステム１００で情報提供管理手段１０において使用者本人を認証処理する場合を前提とする。これを処理条件にして、当該情報提供管理手段１０では図２に示すステップＡ２で使用者の情報処理装置１からの顔画像情報Ｄ１及び個人情報Ｄ２の登録請求が待たれる。

【００４１】この登録請求が有った場合はステップＡ２に移行して情報提供管理手段１０では情報処理装置１によって登録請求された使用者の顔画像情報Ｄ１に個人情報Ｄ２を付加して管理するようになされる。このとき、個人情報Ｄ２には情報提供管理手段１０を含むネットワーク構成用の電子機器を操作できる範囲を示した操作権情報が付加される。こうすると使用者がネットワーク会議参加時等において、マウス操作できる範囲を限定することができる。そして、ステップＡ３に移行して使用者の情報処理装置１に対して登録済みを示すキー情報ＩＤが配信される。その後、ステップＡ８に移行する。

【００４２】また、ステップＡ１で登録請求が無い場合はステップＡ４に移行して、情報処理装置１から当該情報提供管理手段１０へ使用者のキー情報ＩＤ及び個人情報Ｄ２の提示が有ったかがチェックされる。使用者からの認証要求を監視するためである。この提示がない場合はステップＡ１に戻る。

【００４３】使用者の情報処理装置１では登録済みを示すキー情報ＩＤの配信を受けた後は、情報提供管理手段１０に対してＧＵＩ機能を利用してキー情報ＩＤが提示される。このときには、情報処理装置１と情報提供管理手段１０とが通信手段４により接続されていることが前提となる。これを処理条件にして、情報処理装置１に対してステップＡ４で使用者からの認証要求が有った場合は、ステップＡ５に移行して情報提供管理手段１０ではキー情報ＩＤに基づいて顔画像情報Ｄ１から個人情報Ｄ２が読み出され、ここで読み出された個人情報Ｄ２と提示された個人情報Ｄ２とを比較照合して本人を認証するようになされる。

【００４４】従って、顔画像情報Ｄ１から読み出した個人情報Ｄ２と、使用者から提示された個人情報Ｄ２とが一致した場合は当該システムへの参加を許可することができる。また、顔画像情報Ｄ１から読み出した個人情報Ｄ２と、第三者から提示されたような個人情報Ｄ２とが一致しない場合は当該システムへの参加を拒否することができる。これにより、情報提供管理手段１０において、当該情報提供管理手段１０を含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

【００４５】［情報処理系IIで認証処理をする場合②］図３Ａ及びＢは情報処理系IIにおける認証例を示すフローチャートである。このシステム１００で情報処理装置１において使用者本人を認証処理する場合を前提とする。

【００４６】これを処理条件にして情報提供管理手段１０では、図３Ａに示すフローチャートのステップＢ１で使用者の情報処理装置１からの顔画像情報Ｄ１及び個人情報Ｄ２の登録請求が待たれる。

【００４７】この登録請求が有った場合は、ステップＢ２に移行して情報提供管理手段１０では情報処理装置１によって登録請求された使用者の顔画像情報Ｄ１に個人情報Ｄ２を付加した使用者顔画像情報Ｄ０を作成する。個人情報Ｄ２はキー情報ＩＤによって復号可能な情報に暗号化され、暗号化後の個人情報Ｄ２を使用者の顔画像内の上下の所定ラインを表示する画像表示情報に重畳するようになされる。こうすると、個人情報Ｄ２を容易に復号、改ざんできないようにすることができる。

【００４８】そして、ステップＢ３に移行して情報提供管理手段１０から使用者の情報処理装置１に対して使用者顔画像情報Ｄ０及び登録済みを示すキー情報ＩＤが配信される。このとき、使用者顔画像情報Ｄ０及び登録済みを示すキー情報ＩＤはＣＤ－ＲＯＭ等の記憶媒体を利用して配布してもよい。

【００４９】また、情報処理装置１では図３Ｂに示すフローチャートのステップＣ１で使用者顔画像情報Ｄ０＋登録済みを示すキー情報ＩＤを受信（インストール）する。その後、例えば、情報処理装置１と情報提供管理手段１０とを通信手段４により接続してネットワーク電子会議システム等を構築する場合に、ステップＣ２に移行して当該情報処理装置１では当該ＧＵＩ機能を利用したキー情報ＩＤ乃至個人情報Ｄ２が入力されるのを待つ。

【００５０】キー情報ＩＤ乃至個人情報Ｄ２が入力された場合は、ステップＣ３に移行して情報処理装置１ではキー情報ＩＤに基づいて使用者顔画像情報Ｄ０から個人情報Ｄ２が読み出される。ここで読み出された個人情報Ｄ２はステップＣ４で先に提示された個人情報Ｄ２とを比較照合され、本人を認証するようになされる。

【００５１】このシステム１００で使用者顔画像情報Ｄ０を構成する画像表示情報にはチェック情報が含まれ、

使用者の認証時にチェック情報に基づいて画像表示情報の符号ビットを加算し、符号ビットを加算した加算結果とチェック情報による期待加算結果とを比較照合するようになされる。

【００５２】そして、比較照合結果がステップＣ５で液晶ディスプレイ１１に表示される。上述の比較照合の結果で、符号ビットを加算した加算結果とチェック情報による加算結果とが一致しない場合は、当該システムへの使用者の参加を拒否するようになされる。又は、情報提供管理手段１０を含むネットワーク構成用の電子機器の使用権利が制限される。この際の制限に関しては、会議に参加できないようにする、その使用者が未認証であることが他の参加者に容易にわかるような使用者顔画像情報Ｄ０の表示での参加、かつ、チャットやファイル転送等のサービスが受けられない等、使用権を制限するようになされる。

【００５３】このように、本発明に係る実施形態としてのネットワーク情報処理システム１００によれば、当該システムへの参加時等に情報提供管理手段１０又は情報処理装置１において、当該情報処理装置１のＧＵＩ機能を利用して使用者本人を特定するための認証処理がなされる。

【００５４】従って、顔画像情報Ｄ１から読み出した個人情報Ｄ２と、使用者から提示された個人情報Ｄ２とが一致した場合は当該システムへの参加を許可することができる。また、顔画像情報Ｄ１から読み出した個人情報Ｄ２と、第三者から提示された個人情報Ｄ２とが一致しない場合は当該システムへの参加を拒否することができる。これにより、情報提供管理手段１０又は情報処理装置１において、当該情報提供管理手段１０を含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

【００５５】（２）　実施例

図４は本発明に係る実施例としての遠隔地間電子会議システム１０２の構成例を示すイメージ図である。この実施例ではネットワーク情報処理システムの一例となる遠隔地間電子会議システム１０２を構築し、情報提供管理手段で予め使用者顔画像情報Ｄ０を作成し、これを個々の使用者の情報処理装置に配布し、会議システム参加時にユーザの認証するようにしたものである。

【００５６】図４に示す遠隔地間電子会議システム１０２はローカル側の情報処理システム＃１と、リモート側の情報処理システム＃２とが通信手段の一例となるＨＵＢ（集線接続器）９Ａ，９Ｂやゲートウエイ４０，通信ケーブル４０Ａ，４０Ｂ、４１等を通じて接続され、これらの情報処理システム＃１，＃２間において、ユーザ情報を相互に交換するようにしたものである。

【００５７】ローカル側の情報処理システム＃１には情報提供管理手段の一例となるプレゼンテーション装置１０Ａが備えられ、２台のノートパソコンＰＣｉ（ｉ＝１，２）が準備される。プレゼンテーション装置１０Ａは情報提供管理系Ｉを構成し、ノートパソコンＰＣｉは情報処理系IIを構成する。プレゼンテーション装置１０Ａと各々のノートパソコンＰＣ１，ＰＣ２とは無線ＬＡＮ通信方式により接続して使用される。ノートパソコンＰＣ１，ＰＣ２のＧＵＩ機能を利用してプレゼンテーション装置１０Ａを遠隔制御するようになされる。

【００５８】プレゼンテーション装置１０Ａはプロジェクタ２Ａ及びコミュニケータ３Ａを有している。コミュニケータ３Ａはグローバルアドレス（４３．２．５７．１１）及びＩＰアドレス（１９２．１６８．０．１）を有しており、ノートパソコンＰＣ１，ＰＣ２から遠隔操作指示に基づいてプロジェクタ２Ａを含む電子情報処理を支援するようになされる。

【００５９】コミュニケータ３Ａはパーソナルコンピュータ機能を有しており、ノートパソコンＰＣ１，ＰＣ２の入力操作機能によって情報処理をするようになされる。ノートパソコンＰＣ１はＬｏｃａｌ１であり、ノートパソコンＰＣ２はＬｏｃａｌ２である。コミュニケータ３ＡはローカルＨＵＢ９に接続され、通信ケーブル４０Ａ、ゲートウエイ４０及び通信ケーブル４１を通じてリモート側の情報処理システム＃２に接続されている。

【００６０】また、リモート側の情報処理システム＃２には情報提供管理手段の一例となるプレゼンテーション装置１０Ｂが備えられ、２台のノートパソコンＰＣｉ（ｉ＝３，４）が準備される。プレゼンテーション装置１０Ｂも情報提供管理系Ｉを構成し、ノートパソコンＰＣｉも情報処理系IIを構成する。プレゼンテーション装置１０Ｂと各々のノートパソコンＰＣ３，ＰＣ４とは無線ＬＡＮ通信方式により接続して使用される。ノートパソコンＰＣ３，ＰＣ４のＧＵＩ機能を利用してプレゼンテーション装置１０Ｂを遠隔制御するようになされる。

【００６１】プレゼンテーション装置１０Ｂはプロジェクタ２Ｂ及びコミュニケータ３Ｂを有している。コミュニケータ３Ｂはグローバルアドレス（４３．０．２１．１２１）及びＩＰアドレス（１９２．１６８．０．１）を有しており、ノートパソコンＰＣ３，ＰＣ４から遠隔操作指示に基づいてプロジェクタ２Ｂを含む電子情報処理を支援するようになされる。コミュニケータ３Ｂもパーソナルコンピュータ機能を有しており、ノートパソコンＰＣ３，ＰＣ４の入力操作機能によって情報処理をするようになされる。ノートパソコンＰＣ３はＲｅｍｏｔｅ１であり、ノートパソコンＰＣ４はＲｅｍｏｔｅ２である。

【００６２】コミュニケータ３ＢはリモートＨＵＢ９に接続され、通信ケーブル４０Ｂ、ゲートウエイ４０及び通信ケーブル４１を通じてローカル側の情報処理システム＃１に接続されている。この電子会議システム１０２ではローカル側のコミュニケータ３Ａはユーザ情報

として以下の参加者情報、つまり、参加者のノートパソコンＰＣｉのＩＰアドレスを管理する。その参加者情報として、

＜Ｕｓｅｒ名＞　　＜ＩＰアドレス＞
Ｌｏｃａｌ１　　１９２．１６８．０．１２９
Ｌｏｃａｌ２　　１９２．１６８．０．２１４

を管理するようになされる。同様にして、リモート側のコミュニケータ３Ｂはユーザ情報として以下の参加者情報、つまり、参加者のノートパソコンＰＣｉのＩＰアドレスを管理する。その参加者情報としては、

＜Ｕｓｅｒ名＞　　＜ＩＰアドレス＞
Ｒｅｍｏｔｅ１　　１９２．１６８．０．８４
Ｒｅｍｏｔｅ２　　１９２．１６８．０．５３

を管理するようになされる。そして、ローカル側とリモート側とを接続した時は、これらの参加者情報をコミュニケータ３Ａ及び３Ｂ間で交換し合うようになされる。

【００６３】各々のノートパソコンＰＣｉはキー情報の一例となるユーザキーＩＤに基づいて任意の情報を処理する装置である。ユーザキーＩＤは使用者本人を認証するためパスワード等である。会議参加時にはユーザキーＩＤに基づいて使用者顔画像情報Ｄ０の一例となるユーザアイコン画像情報（以下で単にユーザアイコン画像という）から個人情報の一例となるユーザ情報（Ｕｓｅｒ　Ｉｎｆｏｒｍａｔｉｏｎ）Ｄ２を読み出し、このユーザアイコン画像から読み出されたユーザ情報Ｄ２とキーボード１４により入力されたユーザ情報Ｄ２とを比較照合するようになされる。従って、当該ノートパソコンＰＣｉにおいて使用者本人を認証することができる（図１参照）。

【００６４】続いて、コミュニケータ３の内部構成例について説明をする。図５はコミュニケータ３Ａ等の内部構成例を示すブロック図である。コミュニケータ３Ｂについてはコミュニケータ３Ａと同様であるのでその説明を省略する。図５に示すコミュニケータ３Ａはパソコン機能を有しており、ノートパソコンＰＣｉのマウス操作によって情報処理をするものである。使用者のノートパソコンＰＣｉから転送される情報を処理し表示情報を含む電子情報内容を提供するようになされる。

【００６５】コミュニケータ３Ａはデータバス３６を有しており、このデータバス３６にはディスプレイアダプタ３１、ＣＰＵ３２、ワーク用のＲＡＭ３３、データ格納装置３４、ネットアダプタ３５等が接続される。

【００６６】ディスプレイアダプタ３１はプレゼンテーション用の資料を処理して、ＲＧＢ信号を作成する機能を有している。このプレゼンテーション用の資料に基づくＲＧＢ信号はプロジェクタ２Ａ等に出力される。ワーク用のＲＡＭ３３はプライベートＩＰアドレスやプレゼンテーション用の資料に係る転送情報を一時記憶するようになされる。

【００６７】データ格納装置３４は図示しない記憶手段の一例となるハードディスク（ＨＤＤ）、ＲＯＭ及びＲＡＭから構成されている。ハードディスクには少なくとも、ノートパソコンＰＣｉから登録請求された使用者の顔画像情報Ｄ１及びユーザ情報Ｄ２を記憶するようになされる。この他にプレゼンテーション用の資料を格納するようになされる。ＲＯＭには電子会議システムを支援するための制御プログラム（以下システム支援制御プログラムという）が記述されている。システム支援制御プログラムはＣＰＵ３２を動作させるための基本ソフトウェアやプレゼンテーションデータを処理するプログラムから構成されている。

【００６８】ネットアダプタ３５ではノートパソコンＰＣｉからプレゼンテーションデータや各種コマンドの送受信を行うようになされる。ＣＰＵ３２は制御装置の一例であり、システム支援制御プログラムに基づいてディスプレイアダプタ３１、ワーク用のＲＡＭ３３、データ格納装置３４、ネットアダプタ３５等の入出力を制御するようになされる。

【００６９】例えば、ＣＰＵ３２では使用者のノートパソコンＰＣｉによって登録請求された使用者の顔画像情報Ｄ１にユーザ情報Ｄ２を付加して管理すると共に、その使用者のノートパソコンＰＣｉに対して登録済みを示すユーザキーＩＤを配信するようになされる。

【００７０】そして、当該コミュニケータ３ＡのＣＰＵ３２に対してノートパソコンＰＣｉからユーザキーＩＤが提示されたとき、ユーザキーＩＤに基づいて顔画像情報Ｄ１からユーザ情報Ｄ２を読み出し、ここで読み出されたユーザ情報Ｄ２と提示されたユーザ情報Ｄ２とを比較照合して本人を認証するようになされる。従って、情報提供管理系Ｉで認証処理をする①の場合に相当し、当該プレゼンテーション装置１０Ａ等において使用者本人を認証処理することができる（第１の情報提供管理装置）。

【００７１】また、情報処理系IIで認証処理をする②の場合には、少なくとも、データ格納装置３４にはノートパソコンＰＣｉから登録請求された使用者の顔画像情報Ｄ１及びユーザ情報Ｄ２が記憶される。ＣＰＵ３２ではユーザアイコン作成登録プログラム等を使用して、使用者の顔画像情報Ｄ１にユーザ情報Ｄ２を付加してユーザアイコン画像を作成すると共に、このユーザアイコン画像及び登録済みを示すユーザキーＩＤが使用者のノートパソコンＰＣｉに配信される（第２の情報提供管理装置）。

【００７２】従って、当該ノートパソコンＰＣｉにおいてユーザキーＩＤに基づきユーザアイコン画像から読み出したユーザ情報Ｄ２と、提示されたユーザ情報Ｄ２とを比較照合して本人を認証することができる。これにより、ノートパソコンＰＣｉ側で使用者本人を認証できる。

【００７３】図６は使用者固定データＵＣＤのフォーマ

ット例を示すイメージ図である。この例では情報処理系IIで認証処理をする②の場合を想定する。図6に示すデータフォーマット例によれば、４２Ｂｙｔｅｓのユーザ情報Ｄ２に対して、チェック情報の一例となる３Ｂｙｔｅｓのチェックサムが付加され、４５Ｂｙｔｅｓの使用者固定データ（Ｕｓｅｒ　Ｃｏｍｆｉｒｍ　Ｄａｔａ：ＵＣＤ）がＣＰＵ３２によって作成される。４２Ｂｙｔｅｓのユーザ情報Ｄ２は暗号化の対象範囲となる。

【００７４】この使用者固定データＵＣＤの先頭の２ＢｙｔｅｓにはヘッダーＩＤ（Ｈｅａｄｅｒ　ＩＤ）が記述される。ヘッダーＩＤにはヘッダコード（固定値＝０ｘＥＣ）が記述され、通常の参加又はゲスト（Ｇｕｅｓｔ）参加の区別がなされる。なお、ゲストの場合は０ｘ００が記述される。ヘッダコードの後方にはライトコード（Ｒｉｇｈｔ　Ｃｏｄｅ）が記述される。ライトコードには管理者が登録時に設定した会議参加中の操作権に関する内容が記述される。

【００７５】ライトコードは８ビットで表示される［ｂｉｔ７→ｂｉｔ０、７：０］。許否内容は「１」又は「０」であり、「１」で許可を示す。ｂｉｔ７及びｂｉｔ６は予備（Ｒｅｓｅｒｖｅｄ：０）であり、ｂｉｔ５にはコミュニケータのステップアップ設定権の許否内容が記述される。ｂｉｔ４にはプレゼンテーション（Ｐｒｅｓｅｎｔａｔｉｏｎ）操作権の許否内容が記述される。ｂｉｔ３にはプロジェクタ（Ｖｉｅｗｅｒ）へのファイル転送操作の許否内容が記述される。ｂｉｔ２にはプロジェクタの表示切り替え操作の許否内容が記述される。ｂｉｔ１にはチャット操作の許否内容が記述される。ｂｉｔ０にはファイル転送操作の許否内容が記述される。

【００７６】ヘッダーＩＤの後方にはユーザ名（Ｕｓｅｒ　Ｎａｍｅ）の記述欄として１２Ｂｙｔｅｓが割り当てられる。ユーザ名は英数字で最大１２文字まで記述可能となされている。ユーザ名の後方にはフルネーム（Ｆｕｌｌ　Ｎａｍｅ）の記述欄として２０Ｂｙｔｅｓが割り当てられる。フルネームは英数字で最大２０文字まで記述可能となされている。フルネームの後方にはユーザＩＤ（Ｕｓｅｒ　ＩＤ）の記述欄として８Ｂｙｔｅｓが割り当てられる。ユーザＩＤは英数字で最大８文字まで記述可能となされている。ユーザ情報Ｄ２の後方には３Ｂｙｔｅｓのチェックサム（Ｃｈｅｃｋ　Ｓｕｍ）が記述される。

【００７７】図7は顔画像ファイルへの重畳（埋め込み）例を示すイメージ図である。この例ではユーザの顔画像が予め準備される。ユーザの顔部位を予めデジタルカメラで撮影して得た顔画像データ（画像表示情報）が使用される。ユーザアイコン画面Ｑの大きさは縦×横＝５５画素×４５画素であり、ユーザの顔画像は５５×４５画素（Ｐｉｘｃｅｌ）内に収まる程度の２４ビットマップ（Ｂｉｔｍａｐ）画像から成る。このビットマップ画像の１画素はＲ（赤色：１ｂｙｔｅ）、Ｇ（緑色：１ｂｙｔｅ）、Ｂ（青色：１ｂｙｔｅ）の３ｂｙｔｅｓで構成される。

【００７８】この例で暗号化後の使用者固定データＵＣＤは使用者の顔画像内の上下の１ラインを表示する画像表示データの下位ビットに重畳（記述）される。使用者固定データＵＣＤはユーザ情報Ｄ２＋チェックサムから構成される。

【００７９】この例では使用者固定データＵＣＤの最初からｘバイト目を次式（１）のように定義する。

ＵＣＤ［ｘ］［７：０］　　・・・・・・（１）

ユーザの顔画像の大きさが縦×横＝５５画素×４５画素であることから、図6に示したフォーマット例により次式（２）、すなわち、

ＵＣＤ［４４：０］［７：００］
＝（Ｈｅａｄｅｒ　ＩＤ［１：０］［７：０］、
　Ｕｓｅｒ　Ｎａｍｅ［１１：００］［７：００］、
　Ｆｕｌｌ　Ｎａｍｅ［１９：０］［７：００］
　Ｕｓｅｒ　ＩＤ　［７：０］［７：０］
　Ｃｈｅｋ　Ｓｕｍ［２：０］［７：０」　・・・・・・・（２）

となる。

【００８０】また、ｙライン目の左からｘ番目のＲ，Ｇ，Ｂ色の画素データに関してオリジナルデータを次の式（３）ように定義する。

Ｒｏｒｇ［ｘ］［ｙ］［７：０］
Ｇｏｒｇ［ｘ］［ｙ］［７：０］
Ｂｏｒｇ［ｘ］［ｙ］［７：０］　・・・・・・（３）

【００８１】更に、ｙ＝５５ライン目の左からｘ番目のＲ，Ｇ，Ｂ色の画素データの使用者固定データＵＣＤの挿入後のデータを次の式（４）のように定義する。

Ｒ［ｘ］［５５］［７：０］
＝（Ｒｏｒｇ［ｘ］［７：１］、ＵＣＤ［ｘ］［７］）
Ｇ［ｘ］［５５］［７：０］
＝（Ｇｏｒｇ［ｘ］［７：１］、ＵＣＤ［ｘ］［６］）
Ｂ［ｘ］［５５］［７：０］

＝（Ｂｏｒｇ［ｘ］［７：２］、ＵＣＤ［ｘ］［５：４］）・・・（４）

【００８２】また、ｙ＝１ライン目の左からｘ番目のＲ，Ｇ，Ｂ色の画素データの使用者固定データＵＣＤの挿入後のデータを次の式（５）のように定義する。

Ｒ［ｘ］［１］［７：０］
＝（Ｒ［ｘ］［７：１］、ＵＣＤ［ｘ］［３］）
Ｇ［ｘ］［１］［７：０］
＝（Ｇ［ｘ］［７：１］、ＵＣＤ［ｘ］［２］）
Ｂ［ｘ］［１］［７：０］
＝（Ｂ［ｘ］［７：２］、ＵＣＤ［ｘ］［１：０］）・・・・・・（５）

【００８３】この例では３ｂｙｔｅｓのチェックサムについては、ビットマップ画像のＲ、Ｇ、Ｂについて次式（６）のように定義する。

Ｃｈｅｃｋ　Ｓｕｍ［２］［７：０］＝ＣＳＲ［７：０］
Ｃｈｅｃｋ　Ｓｕｍ［１］［７：０］＝ＣＳＧ［７：０］
Ｃｈｅｃｋ　Ｓｕｍ［０］［７：０］＝ＣＳＢ［７：０］・・・・（６）

【００８４】このビットマップ画像のＲ、Ｇ、Ｂ色に係るｘ方向に符号ビットを加算し、ｙライン方向に符号ビットを加算するチェックサムは次式（７）のように定義する。

ＣＳＲ［７：０］
＝Ｒ［ｘ］［ｙ］［７：０］の総和（１←ｘ←４２、１←ｙ←５５）
ＣＳＧ［７：０］
＝Ｇ［ｘ］［ｙ］［７：０］の総和（１←ｘ←４２、１←ｙ←５５）
ＣＳＢ［７：０］
＝Ｂ［ｘ］［ｙ］［７：０］の総和（１←ｘ←４２、１←ｙ←５５）
・・・（７）

【００８５】続いて、ユーザアイコン画像の作成例について説明をする。図８はユーザアイコン画像の作成例を示すフローチャートである。この実施例でユーザが対象となるネットワーク電子会議システムや、ネットワーク教育システム等を利用する場合に、予めシステム管理者にユーザアイコン画像を作成してもらいこれを登録するようになされる。

【００８６】この例ではユーザアイコン画像をシステム管理者のパーソナルコンピュータ（以下でパソコンという）等を使用して作成する場合を想定する。もちろん、システム管理者がコミュニケータ３Ａ等を管理するのであれば、コミュニケータ３Ａ等で作成してもよい。いずれも、会議前日に登録を済ませておくことが好ましい。

【００８７】これを処理条件にしてシステム管理者のパソコン又はコミュニケータ３Ａ等では、図８に示すフローチャートのステップＥ１で使用者のノートパソコンＰＣｉからの顔画像情報Ｄ１及びユーザ情報Ｄ２のアイコン登録請求が待たれる。

【００８８】このアイコン登録請求が有った場合は、ステップＥ２に移行してコミュニケータ３Ａ等ではノートパソコンＰＣｉによって登録請求された使用者の顔画像情報Ｄ１にユーザ情報Ｄ２を付加したユーザアイコン画像を作成する。なお、ステップＥ２～Ｅ８はシステム管理者におけるアイコン作成登録プログラムが使用される。

【００８９】このとき、管理者はユーザから顔写真、ユーザキーＩＤ（キー情報）、ユーザ名，フルネーム，ユーザＩＤを入手する。ここで、ユーザＩＤには社員番号、電話番号、部課コードなどが使用される。管理者はこれらの情報に加え、アイコン登録請求者（ユーザ）にシステム１０２上、どこまで操作権を許可するかを設定する。この設定は使用者固定データＵＣＤのライトコードにその内容を記述することで制限するようになされる。

【００９０】この際に、システム管理者のパソコン又はコミュニケータ３Ａ等ではヘッダーコード（２ｂｙｔｅｓ：０ｘＥＣ＊＊）、＊＊はライトコード（１ｂｙｔｅ）、ユーザ名（１２ｂｙｔｅｓ：英数字１２文字）、フルネーム（２０ｂｙｔｅｓ：英数字２０文字）及びユーザＩＤ（８ｂｙｔｅｓ：英数字８文字）で構成されるユーザ情報Ｄ２（４２ｂｙｔｅｓ）が作成される。

【００９１】その後、ステップＥ３でユーザ情報Ｄ２はユーザキーＩＤ（パスワード）に基づいて復号可能な暗号化される。暗号アルゴリズムには共有鍵方式（ＤＥＳなど）が使用される。ユーザは、会議参加時等において、当該システム１０２にログインするときにこのユーザキーＩＤを入力して正規に登録されたユーザであることをチェックされる。

【００９２】そして、ステップＥ４に移行して暗号化後のユーザ情報Ｄ２は、図７に示したユーザアイコン画面Ｑ内に重畳される。ユーザ情報Ｄ２は顔画像が劣化しないように、かつ目立たない位置に埋め込まれる。この例では、ユーザアイコン画面Ｑの上下１ラインを表示するＲ，Ｇ，Ｂ色の画像データの下位ビットに埋め込まれ

る。こうすると、ユーザ情報Ｄ２を容易に復号、改ざんできないようにすることができる。

【００９３】その後、ユーザアイコン画面Ｑに埋め込まれた画像データに対する、Ｒ，Ｇ，Ｂ色のそれぞれのチェックサムをステップＥ５で計算し、Ｒ，Ｇ，Ｂ色に係るチェックサムをステップＥ６で再度、顔画像データに埋め込む。顔画像データが改ざんされた場合は、このチェックサムのチェック機能で判別することができる。

【００９４】そして、ステップＥ７では作成されたファイル名は、ユーザ名に関連した名前で登録される。システム管理者のパソコンや、当該システム１０２でコミュニケータ３Ａ等をサーバ装置としたとき、このコミュニケータ３Ａ等に登録する。このようにすることで、ステップＥ８で常にコミュニケータ３Ａ等からユーザアイコン画像及び登録済みを示すユーザキーＩＤを参照又は発行（配信）できるようになる。

【００９５】この場合、常にサーバ装置等にアクセスできる環境でしかシステム１０２が稼動できなくなってしまうため、そのような場合には、アイコン登録請求者に対してＣＤ－ＲＯＭ等の記憶媒体にユーザアイコン画像を記録し手渡して発行し、使用者のノートパソコンＰＣｉ上に置くことも可能である。

【００９６】図９はノートパソコンＰＣｉにおける起動時のＧＵＩ操作画面（以下でＧＵＩ起動時画面という）Ｐ０の表示例を示すイメージ図である。図９に示すＧＵＩ起動時画面Ｐ０は起動時にノートパソコンＰＣ１に表示されるものであり、クライアントＧＵＩプログラムに基づく表示例である。ＧＵＩ起動時画面Ｐ０では２分割表示方式が採られる。当該画面Ｐ０の左側にはＧＵＩ操作画面（以下でコントロール画面という）Ｐ１が表示され、画面右側にはアテンディ画面Ｐ２が表示される。この例で、コントロール画面Ｐ１にはスクリーン・スナップモードによる選択画面が表示される。

【００９７】コントロール画面Ｐ１において、中央にはデバイスアイコン用のエリア２１が設けられ、プロジェクタ等のアイコンが表示される。このエリア２１の上部にはスクリーンスナップモード時の「ｓｔａｒｔ」や、「ｓｔｏｐ」ボタンＫ０が表示される。その右隣にはアテンディボタンＫ１が表示され、その上方には「ＨＥＬＰ」ボタンＫ２が表示され、このコントロール画面Ｐ１の外枠上部には「閉じる」ボタンＫ３が表示されている。エリア２１の下方には「ファイル・エクスプローラ／ヒストリ」用のタブＫ４が表示され、このタブＫ４内にはファイルリストエリア２２を表示するようになされる。なお、コントロール画面Ｐ１の左側上部には企業イメージのロゴマーク１９を表示できるようになされている。

【００９８】アテンディ画面Ｐ２において、中央にはアテンディユーザリスト用のエリア２３が設けられ、会議参加者や、そのノートパソコンＰＣｉのＩＰアドレス等がアイコンと共に表示される。このエリア２３の上部にはユーザ情報エリア２４が設けられ、使用者固定データＵＣＤに基づくユーザアイコン画像が表示される。この他に、ユーザ情報エリア２４にはローカル側で特定のノートパソコンＰＣｉのＩＰアドレス等を表示するようになされる。アテンディ画面Ｐ２の右側上部には「チャット」ボタンＫ５が表示される。また、アテンディ画面Ｐ２の下方にはローカルボタンＫ６、リモートボタンＫ７及びクリアボタンＫ８等を表示するようになされる。

【００９９】図１０はアテンディ画面Ｐ２におけるユーザアイコン画像の表示例を示すイメージ図である。図１０に示すアテンディ画面Ｐ２によれば、ユーザ情報エリア２４にはユーザアイコン画像が表示される。この例では会議参加が許可されたユーザの顔画像、ユーザ名○○○、当該ノートパソコンＰＣｉのＩＰアドレスとして４３．２．５７．１９３が表示される。なお、アテンディユーザリスト用のエリア２３にはＲｅｍｏｔｅの会議参加者の顔画像、ユーザ名×××、当該ノートパソコンＰＣｉのＩＰアドレスとして１９２．１６８．０．２２２が表示される。

【０１００】図１１はコントロール画面Ｐ１におけるファイル確認画面Ｐ１１の表示例を示すイメージである。図１１に示すファイル確認画面Ｐ１１によれば、不特定多数の使用者、つまり、別の参加者が当該ノートパソコンＰＣｉを使用して会議に参加しようとする場合である。この場合はユーザフォトに関してファイル確認画面Ｐ１１を開き、ユーザ名×××を入力すると、それに関連した画像ファイルのリストが表示される。

【０１０１】このリストの中からユーザ名×××を選択（クリック）すると、リストの隣の所定の表示領域にＲｅｍｏｔｅの会議参加者の顔画像が表示される。ユーザ名はファイル名と共にファイルの種類を指定することで当該ノートパソコンＰＣｉ内に保存される。Ｒｅｍｏｔｅ側の会議参加者がローカル側に出向して会議に参加する場合が考えられるためである。

【０１０２】図１２はコントロール画面Ｐ１におけるセットアップ画面Ｐ１２の表示例を示すイメージ図である。図１２に示すセットアップ画面Ｐ１２はファイル確認画面Ｐ１１でユーザ名×××を選択することで表示切替されたアイコン画面である。このセットアップ画面Ｐ１２にはＵＳＥＲ　ＮＡＭＥ　×××や、ＵＳＥＲ　ＰＨＯＴＯ（４５×５５ｐｉｘｅｌｓ）として、Ｒｅｍｏｔｅの会議参加者の顔画像が表示されると共に、ＵＳＥＲ　ＫＥＹが表示される。ＵＳＥＲ　ＫＥＹにはパスワード「＊＊＊＊＊＊＊」を入力するようになされる。セットアップ画面Ｐ１２にはこの他に閲覧キー（ＢＲＯＷＳＥ）Ｋ９や、ＯＫキーＫ１０やキャンセルキーＫ１１が表示される。パスワードが正しければ、Ｒｅｍｏｔｅの会議参加者がローカル側の会議に参加できるようになる。

【０１０３】図１３はアテンディ画面Ｐ２における制限付きユーザアイコン画像の表示例を示すイメージ図である。図１３に示すアテンディ画面Ｐ２によれば、ユーザ情報エリア２４には制限付きユーザアイコン画像が表示される。この例では会議参加を許可されたが操作権が制限されるゲスト（Ｇｕｅｓｔ）、ユーザ名△△△、その者のノートパソコンＰＣｉのＩＰアドレスとして１９２．１６８．０．２４６が表示される。なお、アテンディユーザリスト用のエリア２３にはＲｅｍｏｔｅの会議参加者の顔画像、ユーザ名×××、当該ノートパソコンＰＣｉのＩＰアドレスとして１９２．１６８．０．２２２が表示されている。

【０１０４】図１４及び図１５は遠隔地間電子会議システム１０２の会議参加時のノートパソコンＰＣｉにおける処理例（その１、２）を示すフローチャートである。この実施例ではローカル側において、ユーザが会議に参加する場合の流れを示している。例えば、ノートパソコンＰＣｉとコミュニケータ３Ａ等とを通信手段４により接続して遠隔地間電子会議システム１０２等に参加する場合を想定する。

【０１０５】この例ではいずれの使用者のユーザアイコン画像＋登録済みを示すユーザキーＩＤは予め当該ノートパソコンＰＣｉにインストールされているものとする。このシステム１０２でユーザアイコン画像を構成する画像表示情報にはチェック情報（Ｃｈｅｃｋ　Ｓｕｍ）が含まれ、ユーザの認証時にチェック情報に基づいて本人を認証する場合を例に挙げる。これを処理条件にして、前回のユーザが今回も当該ノートパソコンＰＣｉを使用する場合及び、リモート側の使用者がローカル側に出向してこのＰＣｉを使用する場合に分けて説明をする。なお、ゲストの場合はリモート側で既にユーザアイコン画像が登録されている場合を想定する。

【０１０６】［前回のユーザが今回も当該ＰＣｉを使用する場合］前回のユーザが今回も当該電子会議システム１０２に参加する場合は、既にセットアップが済んでいる。そして、ノートパソコンＰＣｉでは図１４に示すフローチャートのステップＦ１でクライアントＧＵＩプログラムが起動されると、図９に示したようなＧＵＩ起動時画面Ｐ０が液晶ディスプレイ１１に表示される。

【０１０７】ここでステップＦ２で当該ノートパソコンＰＣｉでは前回と同じユーザ名か否かによって制御を分岐するようになるが、今回、ノートパソコンＰＣｉを使用するユーザが前回の使用した人と同じであることから、ステップＦ５に移行して自分のユーザ名とアイコン画像が表示される。このとき、図１０に示すアテンディ画面Ｐ２によれば、ユーザ情報エリア２４にはユーザアイコン画像が表示される。この例では会議参加が許可されたユーザの顔画像、ユーザ名○○○、当該ノートパソコンＰＣｉのＩＰアドレスとして４３．２．５７．１９３が表示される。

【０１０８】そして、ステップＦ６で当該ノートパソコンＰＣｉではＧＵＩ機能を利用してユーザキーＩＤ乃至ユーザ情報Ｄ２が入力される。ここでユーザキーＩＤ及びユーザ情報Ｄ２が入力されると、ステップＦ７～ステップＦ１１，Ｆ１４で４２ｂｉｔｓのユーザ情報Ｄ２が確認される。

【０１０９】この例ではステップＦ７でノートパソコンＰＣｉではユーザキーＩＤに基づいてユーザアイコン画像からユーザ情報Ｄ２及びチェック情報が読出（切り出）される。チェックサムの整合性を確認するためである。

【０１１０】このとき、上述した式（７）に基づいてビットマップ画像（画像表示情報）のＲ、Ｇ、Ｂ色に係るｘ方向に符号ビットが加算され、ｙライン方向に符号ビットが加算される。このチェックサムの計算によって、符号ビットを加算した加算結果とチェック情報による期待加算結果とを比較照合するようになされる。この比較照合の結果で、符号ビットを加算した加算結果とチェック情報による加算結果とが一致しない場合は照会結果が不備（ＮＧ）としてステップＦ１４に移行する。

【０１１１】この比較照合が良好（ＯＫ）の場合はステップＦ９に移行してユーザアイコン画像に埋め込まれたユーザ情報Ｄ２が復号化される。そして、ステップＦ１０に移行して復号化後のユーザ情報Ｄ２と、先に登録されたユーザ情報Ｄ２とが比較照合される。ユーザ名の整合性を確認することで、当該ノートパソコンＰＣｉ上でユーザが正規に登録された者であるかが確認することができる。

【０１１２】更に、ステップＦ１１でヘッダーコードの０ｘＥＣがチェックされる。ヘッダーコードの整合性を確認することでローカル側での通常の会議参加か、リモート側からの出向によるゲスト参加等を判別するためである。このとき、ライトコードによりシステム１０２上での操作範囲が決定される。

【０１１３】これらの比較照合結果は液晶ディスプレイ１１に表示するようになされる。ステップＦ１１でヘッダーコードが０ｘＥＣの場合はローカル側における通常の会議参加なので、ステップＦ１２で当該会議システムへの参加が許容される（図１０参照）。そして、ステップＦ１３で当該ノートパソコンＰＣｉでは会議終了か否かがチェックされる。この例では当該ノートパソコンＰＣｉにおいてエグジットキーの押下を検出して会議を終了するようになされる。会議を終了しない場合はステップＦ１２に戻って会議が継続される。

【０１１４】［前回のユーザと異なる使用者（ゲスト）が当該ＰＣｉを使用する場合］例えば、リモート側の使用者が出向してローカル側の電子会議システム１０２で当該ノートパソコンＰＣｉを使用する場合である。この場合にはその使用者のローカル側でのセットアップが済んでいない。そこで、ノートパソコンＰＣｉでは図１４

に示すフローチャートのステップＦ１でクライアントＧＵＩプログラムが起動されると、図９に示したようなＧＵＩ起動時画面Ｐ０が液晶ディスプレイ１１に表示される。

【０１１５】ステップＦ２では前回と同じユーザ名か否かによって制御を分岐するようになるが、今回、ノートパソコンＰＣｉを使用するユーザが前回のユーザと異なることから、ステップＦ４に移行する。このステップＦ４でユーザ名×××を入力すると、ユーザフォトに関して図９に示したＧＵＩ起動時画面Ｐ０から図１１に示すファイル確認画面Ｐ１１が開かれ、ユーザ名×××に関連した画像ファイルのリストが表示される。

【０１１６】このリストの中でユーザ名×××を選択（クリック）すると、リストの隣の所定の表示領域にリモート側で予めセットアップが済んでいる会議参加者の顔画像が表示される。この顔画像に関してはサーバ装置又は自機にすでに登録されているユーザアイコンファイルのうち、ユーザ名の文字列を含むファイル名のビットマップファイルに基づいてリスト表示される。

【０１１７】そして、ファイル名と共にファイルの種類を指定することで当該ノートパソコンＰＣｉ内に保存される。図１１示したファイル確認画面Ｐ１１から図１２に示すセットアップ画面Ｐ１２へ表示切替がなされる。このセットアップ画面Ｐ１２にはＵＳＥＲ　ＮＡＭＥ　×××や、ＵＳＥＲ　ＰＨＯＴＯ（４５×５５ｐｉｘｅｌｓ）として、Ｒｅｍｏｔｅの会議参加者の顔画像が表示されると共に、ＵＳＥＲ　ＫＥＹが表示される。ＵＳＥＲ　ＫＥＹにはパスワード「＊＊＊＊＊＊＊」を入力するようになされる。

【０１１８】これにより、リモート側の使用者のローカル側でのセットアップが終了する。今回のようにリモート側の会議参加者がローカル側に出向して電子会議システム１０２に参加する場合（ゲスト）が考えられるためである。なお、参加資格のない未登録者の場合はリスト表示がなされない。

【０１１９】その後、ステップＦ５で図１３に示したアテンディ画面Ｐ２にゲストのユーザアイコン画像が表示される。図１３に示すアテンディ画面Ｐ２によれば、ユーザ情報エリア２４には制限付きユーザアイコン画像が表示される。この例では会議参加を許可されたが操作権が制限されるゲスト（Ｇｕｅｓｔ）、ユーザ名△△△、その者のノートパソコンＰＣｉのＩＰアドレスとして１９２．１６８．０．２４６が表示される。

【０１２０】そして、ステップＦ６で当該ノートパソコンＰＣｉでは当該ＧＵＩ機能を利用してユーザキーＩＤ乃至ユーザ情報Ｄ２が入力される。その後、ステップＦ７に移行してノートパソコンＰＣｉではユーザキーＩＤに基づいてユーザアイコン画像からユーザ情報Ｄ２及びチェック情報が読み出される。チェックサムの整合性を確認するためである。

【０１２１】このとき、画像表示情報の符号ビットを加算し、符号ビットを加算した加算結果とチェック情報による期待加算結果とを比較照合するようになされる。この比較照合の結果で、符号ビットを加算した加算結果とチェック情報による加算結果とが一致しない場合は照会結果が不備（ＮＧ）としてステップＦ１４に移行する。

【０１２２】この比較照合が良好（ＯＫ）の場合はステップＦ９に移行してユーザアイコン画像に埋め込まれたユーザ情報Ｄ２が復号化される。そして、ステップＦ１０に移行して復号化後のユーザ情報Ｄ２と、先に登録されたユーザ情報Ｄ２とが比較照合される。ユーザ名の整合性を確認することで、当該ノートパソコンＰＣｉ上でユーザが正規に登録された者であるかが確認することができる。

【０１２３】更に、ステップＦ１１でヘッダーコードの０ｘＥＣがチェックされる。この場合はリモート側からの出向によるゲスト参加であって、ステップＦ１５でヘッダーコードが０ｘ００であることから、ライトコードによりシステム１０２上での操作範囲が制限される。ステップＦ１５ではコミュニケータ３Ａ等を含むネットワーク構成用の電子機器の使用権利が制限される。この際の制限に関しては、その使用者が未認証であることが他の参加者に容易にわかるようなユーザアイコン画像の表示での参加、かつチャット、ファイル転送等のサービスが受けられない等、使用権を制限するようになされる。

【０１２４】このようにＧｕｅｓｔとして操作権が限定された状態で電子会議システムに参加できるようになる（図１３参照）。そして、ステップＦ１６で当該ノートパソコンＰＣｉでは会議終了か否かがチェックされる。この例では当該ノートパソコンＰＣｉにおいてエグジットキーの押下を検出して会議を終了するようになされる。会議を終了しない場合はステップＦ１５に戻って会議が継続される。

【０１２５】なお、ステップＦ８で照会結果がＮＧの場合、ステップＦ１０でユーザ名が異なっている場合及びヘッダーコードが０ｘＥＣではない場合はステップＦ１４に移行してヘッダーコードが０ｘ００であるか否かがチェックされる。ヘッダーコードが０ｘ００はもとより何も記述されていない場合は、ステップＦ１７に移行して当該システム１０１への使用者の参加を拒否するようになされる。当該電子会議システム１０２に参加できないようにするためである。これにより、ユーザアイコン画像を特定のユーザにしか使用できない機構を構築することができる。

【０１２６】このように、本発明に係る実施例としての遠隔地型電子会議システム１０２及びその情報処理方法によれば、当該システム１０２への参加時等にコミュニケータ３Ａ等又はノートパソコンＰＣｉにおいて、当該ノートパソコンＰＣｉのＧＵＩ機能を利用して使用者本人を特定するための認証処理がなされる。

【０１２７】従って、顔画像情報Ｄ１から読み出したユーザ情報Ｄ２と、使用者から提示されたユーザ情報Ｄ２とが一致した場合は当該システム１０２への参加を許可することができる。また、顔画像情報Ｄ１から読み出したユーザ情報Ｄ２と、第三者から提示されたユーザ情報Ｄ２とが一致しない場合は当該システムへの参加を拒否することができる。これにより、コミュニケータ３Ａ等又はノートパソコンＰＣｉにおいて、当該コミュニケータ３Ａ等を含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

【０１２８】この実施例ではネットワーク情報処理システムに関して遠隔地間電子会議システムについて説明したが、これに限られることはなく、ネットワーク教育システム、ネットワークゲームシステム等においても、当該情報提供管理系Ｉを含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

【０１２９】

【発明の効果】以上説明したように、本発明に係るネットワーク情報処理システムによれば、任意の情報を処理する一以上の情報処理装置と、表示情報を含む電子情報内容を提供する情報提供管理手段とが通信手段により接続され、情報提供管理手段又は情報処理装置において、当該情報処理装置の入力操作機能を利用して使用者本人を特定するための認証処理をするものである。

【０１３０】この構成によって、顔画像情報から読み出した個人情報と、使用者から提示された個人情報とが一致した場合は当該システムへの参加を許可することができる。また、顔画像情報から読み出した個人情報と、不正使用者（第三者）から提示された個人情報とが一致しない場合は当該システムへの参加を拒否することができる。従って、情報提供管理手段又は情報処理装置において、当該情報提供管理手段を含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

【０１３１】本発明に係る第１の情報提供管理装置によれば、使用者の顔画像情報に個人情報を付加して管理すると共に、この使用者の情報処理装置に対して登録済みを示すキー情報を配信する制御装置を備え、当該制御装置に対して情報処理装置からキー情報が提示されたとき、このキー情報に基づいて顔画像情報から読み出した個人情報と、提示された個人情報とを比較照合して本人を認証するようにしたものである。

【０１３２】この構成によって、当該情報提供管理装置において使用者本人を認証処理することができる。これにより、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムに対して当該情報提供管理装置を十分応用することができる。

【０１３３】本発明に係る第２の情報提供管理装置によれば、使用者の顔画像情報に個人情報を付加して使用者顔画像情報を作成すると共に、この使用者顔画像情報を及び登録済みを示すキー情報を使用者の情報処理装置へ配信する制御装置を備えるものである。

【０１３４】この構成によって、当該情報処理装置においてキー情報に基づき使用者顔画像情報から読み出した個人情報と、提示された個人情報とを比較照合して本人を認証することができる。従って、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムに対して第２の情報提供管理装置を十分応用することができる。

【０１３５】本発明に係る情報処理装置によれば、キー情報に基づいて任意の情報を処理する場合に使用者本人を認証する制御装置を備え、この制御装置はキー情報に基づいて使用者顔画像情報から個人情報を読み出し、この使用者顔画像情報から読み出された個人情報と入力手段により入力された個人情報とを比較照合するようになされる。

【０１３６】この構成によって、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムに対して当該情報処理装置を十分応用することができる。

【０１３７】本発明に係る情報処理方法によれば、入力操作機能を有して任意の情報を処理する一以上の情報処理系と、少なくとも、情報処理系から転送される情報を処理し表示情報を含む電子情報内容を提供する情報提供管理系とを準備し、これらの情報提供管理系又は情報処理系において、当該情報処理系の入力操作機能を利用して使用者本人を特定するための認証処理をするようになされる。

【０１３８】この構成によって、顔画像情報から読み出した個人情報と、使用者から提示された個人情報とが一致した場合は当該システムへの参加を許可することができる。また、顔画像情報から読み出した個人情報と、不正使用者（第三者）から提示された個人情報とが一致しない場合は当該システムへの参加を拒否することができる。従って、情報提供管理系又は情報処理系において、当該情報提供管理系を含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

【０１３９】この発明はネットワーク会議システムや、ネットワーク教育システム、ネットワークゲームシステム等に適用して極めて好適である。

【図面の簡単な説明】

【図１】本発明に係る実施形態としてのネットワーク情報処理システム１００の構成例を示すブロック図である。

【図２】情報提供管理系Ｉにおける認証例を示すフローチャートである。

【図３】Ａ及びＢは情報処理系IIにおける認証例を示すフローチャートである。

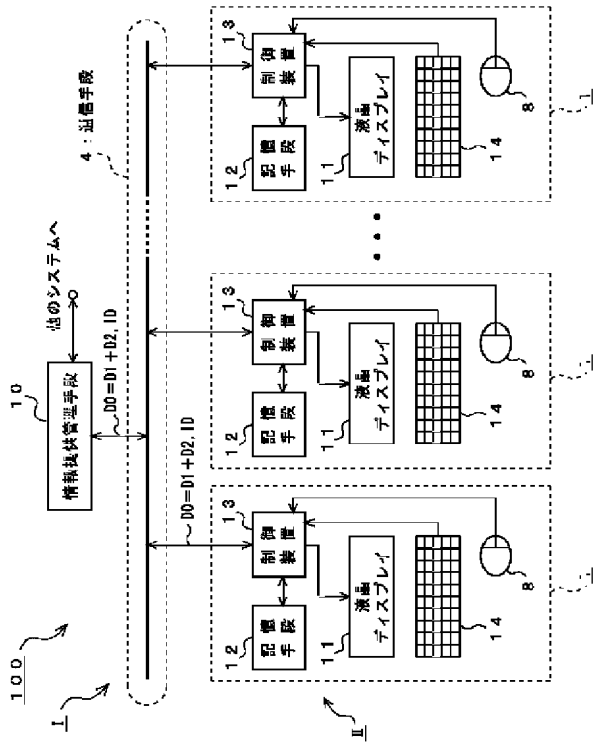
【図４】本発明に係る実施例としての遠隔地間電子会議システム１０２の構成例を示すイメージ図である。

【図５】コミュニケータ３Ａ等の内部構成例を示すブロ

ック図である。
【図６】使用者固定データＵＣＤのデータフォーマット例を示すイメージ図である。
【図７】顔画像ファイルＱへの重畳（埋め込み）例を示すイメージ図である。
【図８】ユーザアイコン画像の作成例を示すフローチャートである。
【図９】ノートパソコンＰＣｉにおけるＧＵＩ起動時画面Ｐ０の表示例を示すイメージ図である。
【図１０】アテンディ画面Ｐ２におけるユーザアイコン画像の表示例を示すイメージ図である。
【図１１】コントロール画面Ｐ１におけるファイル確認画面Ｐ１１の表示例を示すイメージである。
【図１２】コントロール画面Ｐ１におけるセットアップ画面Ｐ１２の表示例を示すイメージ図である。
【図１３】アテンディ画面Ｐ２における制限付きユーザアイコン画像の表示例を示すイメージ図である。
【図１４】遠隔地間電子会議システム１０２への会議参加時のノートパソコンＰＣｉにおける処理例（その１）を示すフローチャートである。
【図１５】その会議参加時のノートパソコンＰＣｉにおける処理例（その２）を示すフローチャートである。
【符号の説明】
１・・・情報処理装置、２Ａ，２Ｂ・・・プロジェクタ、３Ａ，３Ｂ・・・コミュニケータ、４，４０・・・通信手段、８・・・マウス、１０Ａ，１０Ｂ・・・プレゼンテーション装置（情報提供管理手段）、１１・・・液晶ディスプレイ（表示手段）、１２・・・記憶手段、１３・・・制御装置、１４・・・キーボード、３２・・・ＣＰＵ（制御装置）、３４・・・データ格納装置（記憶手段）、１００・・・ネットワーク情報処理システム、１０２・・・遠隔地間電子会議システム、ＰＣｉ（ｉ＝１～ｎ）・・・ノートパソコン（情報処理装置）

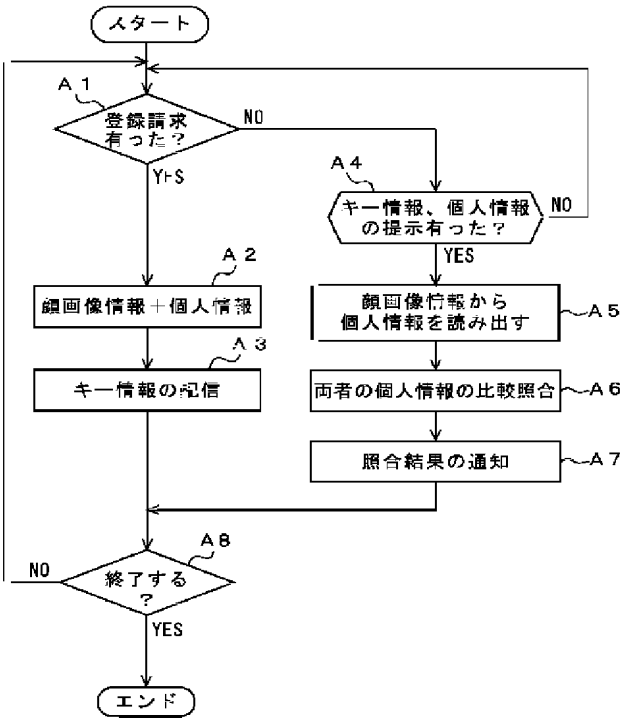
【図１】

実施形態としてのネットワーク情報処理システム１００の構成例



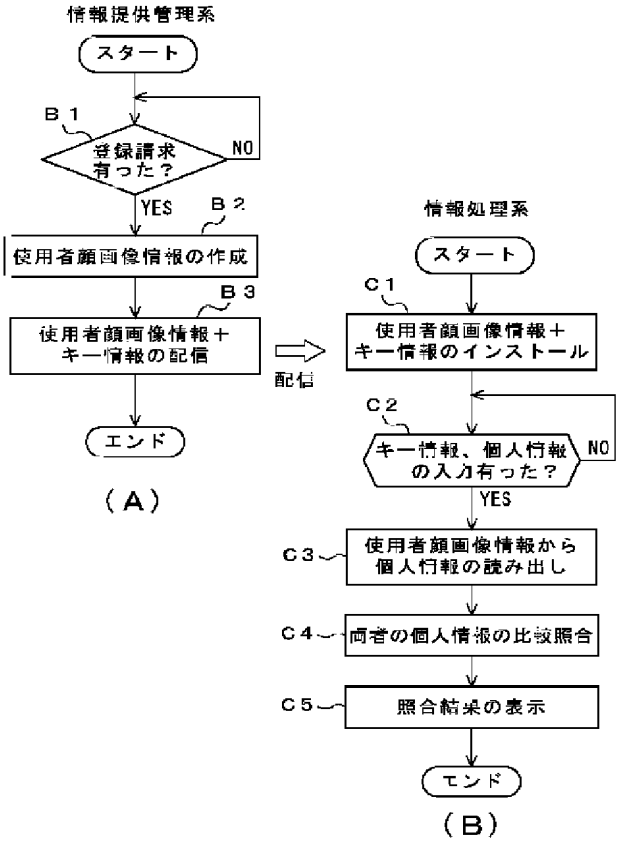
【図２】

情報提供管理系Ｉにおける認証例



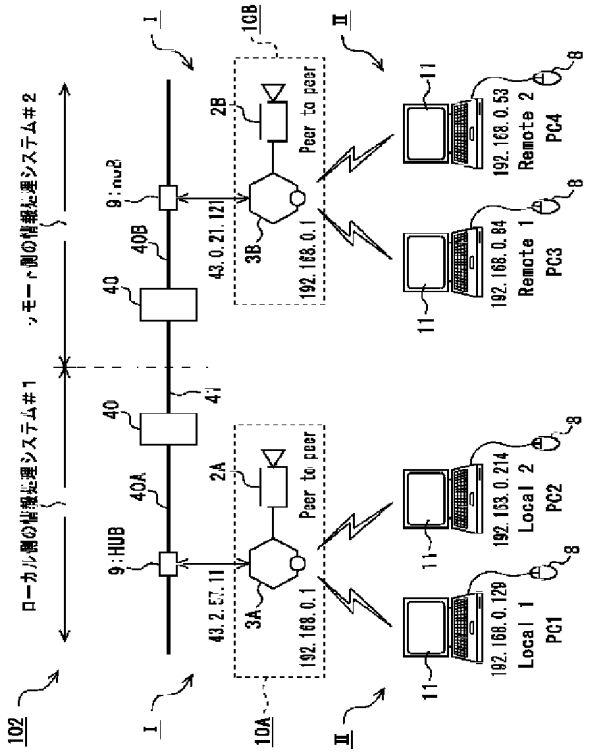
【図3】

情報処理系Iにおける認証例



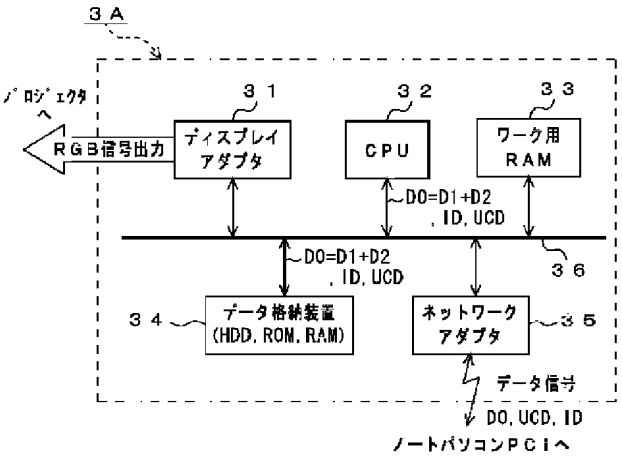
【図4】

遠隔地間電子会議システム１０２の構成例



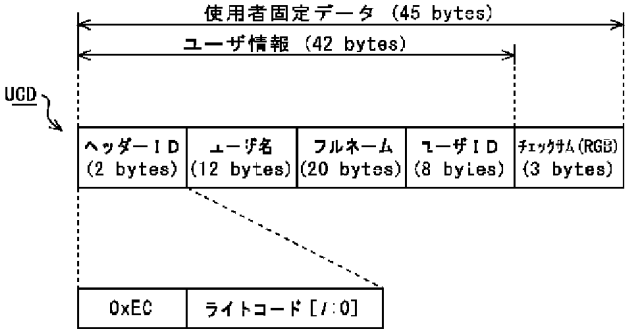
【図5】

コミュニケータ３Ａ等の内部構成例



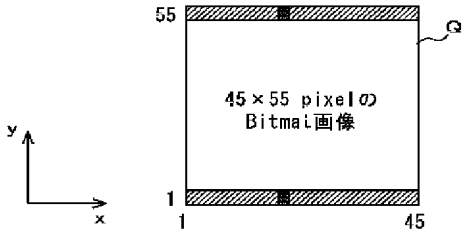
【図6】

使用者固定データＵＣＤのデータフォーマット例



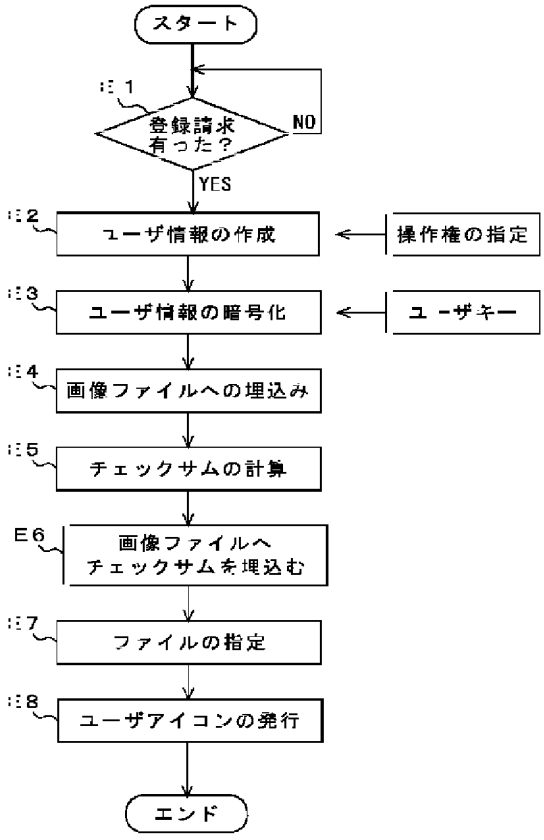
【図7】

顔画像ファイルQへの重畳(埋め込み)例



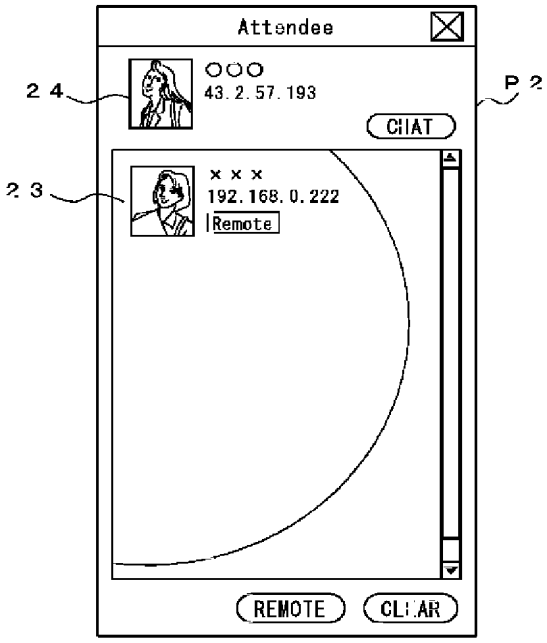
【図8】

ユーザアイコン画像の作成例



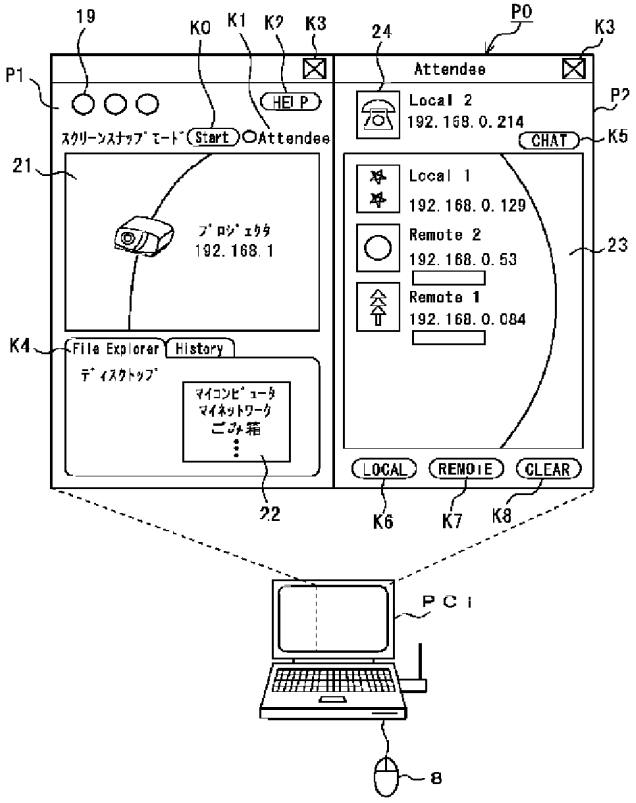
【図10】

アテンディ画面P2における
ユーザアイコン画像の表示例



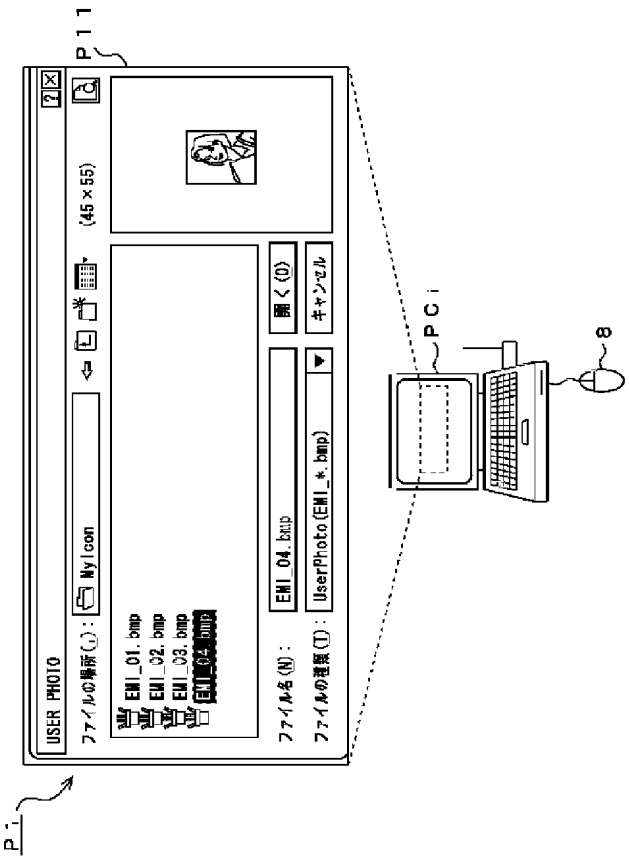
【図９】

ノートパソコンＰＣｉにおけるＧＵＩ
起動時画面Ｐ０の表示例



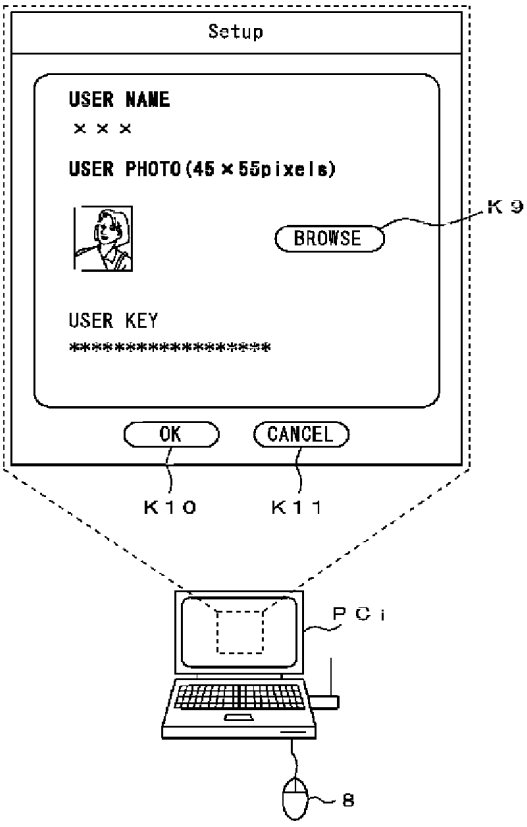
【図１１】

ファイル確認画面Ｐ１１の表示例



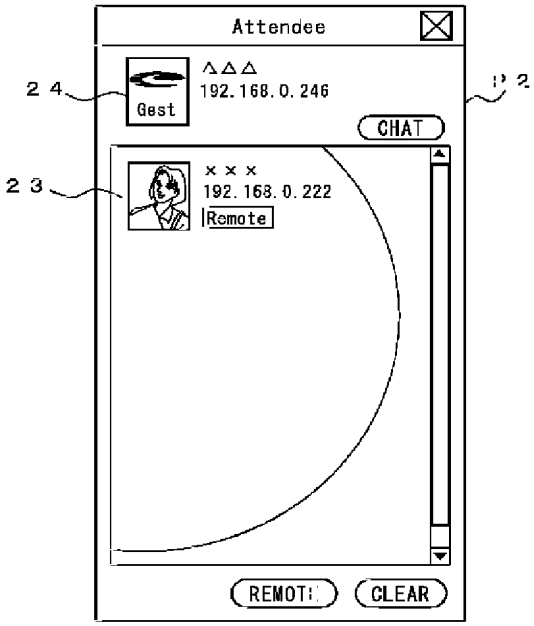
【図１２】

セットアップ画面Ｐｉ２の表示例



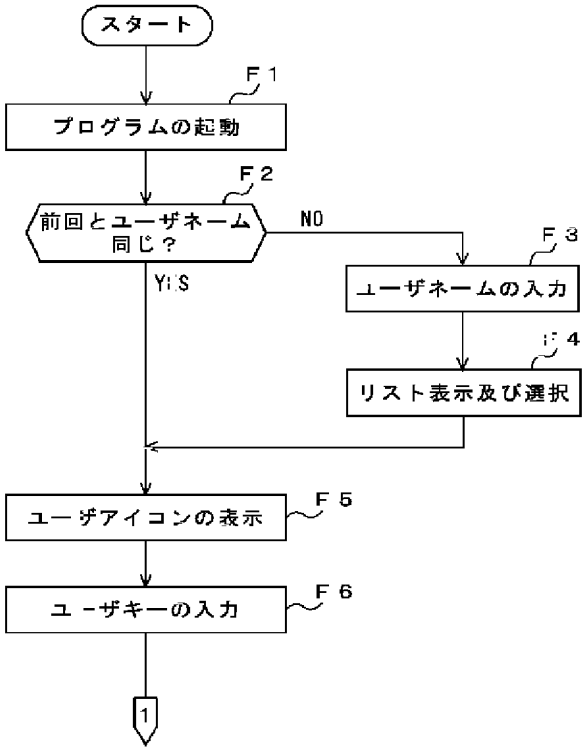
【図１３】

アテンディ画面Ｐ２における制限付き
ユーザアイコン画像の表示例



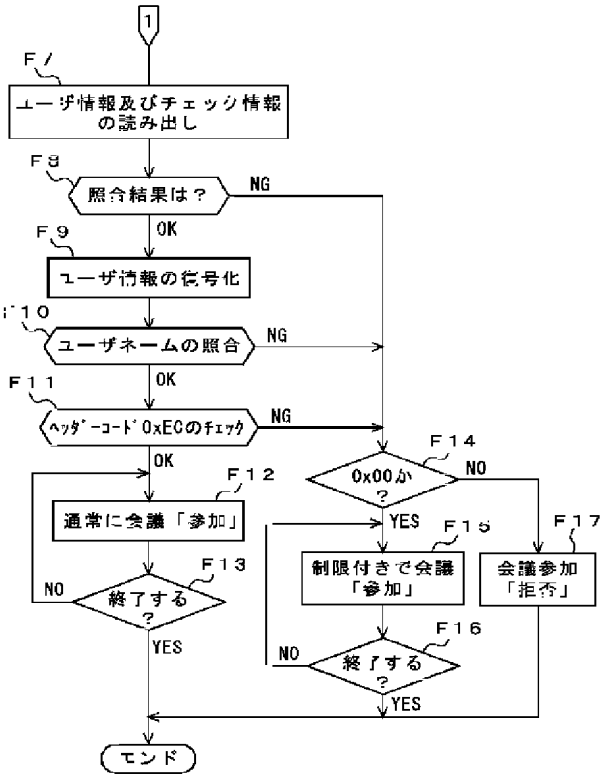
【図14】

ノートパソコンＰＣｉにおける処理例（その１）



【図15】

ノートパソコンＰＣｉにおける処理例（その２）



フロントページの続き

Ｆターム(参考)　5B057 CA01 CA08 CA12 CA16 CB01
CB08 CB12 CB16 CC02 CE08
5B085 AA08 AE23 AE25 BA07 BE04
BE07 BG01 BG02 BG07
5C064 AA02 AB03 AC08 AC22 AD06
BB07 BC23